PART 500 - GENERAL

500.0 Purpose.

500.1 Authorities.

500.2 Policy.

500.3 Definition.

PART 500 - GENERAL

500.0 Purpose.

(a) To provide a central reference of policies for integrating information resources and information technology into the business, mission, goals, and objectives of the Natural Resources Conservation Service (NRCS).

(b) General Manual, Section 270 contains NRCS policy for information technology and information resources management. It establishes the information technology and information resources decision structure for NRCS, conveys specific NRCS policies, and provides references to related NRCS guidelines, Departmental regulations, and other applicable guidance.

500.1 Authorities.

(a) Clinger-Cohen Act of 1996, Public Law 104-106.

(b) Federal Acquisition Reform Act (FARA).

(c) Government Paperwork Elimination Act (GPEA), Public Law 105-277, October 1998.

(d) Management of Federal Information Resources, Office of Management and Budget (OMB) Circular A-130.

(e) Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995.

(f) Privacy Act of 1974, 5 U.S.C. 552a.

500.2 Policy.

(a) All organizational units within NRCS will manage information technology and information resources within the framework and mandates contained in, or referenced in, General Manual, Section 270, and in departmental directives.

(b) Information Resources Management (IRM) will be the terminology used to define the management of information resources and information technology.

500.3 Definition.

(a) Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management,

movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software firmware and similar procedures, services, and related resources.

(b) Information Resources (IR). Resources such as personnel, equipment, data, funds, and information technology necessary to accomplish the mission of the agency and to improve agency performance.

(c) Information Resources Management (IRM). The management of information technology and information resources.

(d) Departmental Information Resources Management Directives. Guidelines published by the USDA, Office of the Chief Information Officer. They are established whenever the Department determines there is a need and no applicable Federal standard exists. USDA directives communicate official policy and procedures to USDA personnel. Directives are classified as permanent (departmental regulations and departmental manuals) and temporary (notices, Secretary's memoranda, and Secretary's announcements.

PART 501 - IRM ORGANIZATIONS: ROLES AND RESPONSIBILITIES

SUBPART A - ORGANIZATIONAL UNITS

PART 501 - IRM ORGANIZATIONS: ROLES AND RESPONSIBILITIES

SUBPART A - ORGANIZATIONAL UNITS

501.0 Purpose.

To describe the overall policy, management, and oversight responsibilities of the Information Technology Division, the Information Technology Center, the National Cartography and Geospatial Center, Deputy Chiefs, Regional offices, State offices, and other offices.

501.1 Authorities.

(a) Chief Financial Officers Act (CFO Act).

(b) Federal Acquisition Streamlining Act (FASA).

(c) Freedom to E-file, Public Law 106-222, June 2000.

(d) Government Paperwork Elimination Act (GPEA), Public Law 105-277, October 1998.

(e) Government Performance and Results Act (GPRA) of 1993, Public Law 103-62.

(f) Clinger-Cohen Act of 1996, Public Law 104-106.

(g) Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995.

(h) Departmental Long-Range IRM Planning, USDA Departmental Regulation (DR) 3111-001, February 1989.

501.2 Policy.

NRCS will organize its information technology staffs to most efficiently support the business needs of the agency. Toward this objective, it is NRCS policy that information technology staffs be decentralized to ensure adequate IRM support and assistance to local users. Local information technology staffs are the primary sources of IRM assistance.

501.3 Responsibilities.

(a) The Chief will:

(1) Assign a Chief Information Officer (CIO) and responsibility to the CIO for maintaining the information technology infrastructure for NRCS.

(2) Ensure that NRCS has an Information Resources Management Review Board that follows policy for IT activities. Reviews and approves specific IT actions to assure that information technology activities reflect the goals and priorities of NRCS programs.

(b) The NRCS CIO will:

(1) Be accountable to the Chief of the Natural Resources Conservation Service (NRCS) and report directly to the NRCS Deputy Chief for Management. The NRCS CIO serves as liaison to the Office of the Chief Information Officer, USDA. The CIO also serves as the Information Technology Division (ITD) Director and provides leadership and guidance for the Information Technology Center (ITC).

(2) Provide national leadership for a comprehensive and effective information technology program that meets the needs of the agency. The CIO is responsible for the information technology activities at both ITD and ITC. The CIO also serves as the overall coordinator for agency information technology activities to ensure maximum efficiency and effectiveness in meeting business needs and requirements.

(3) Provide national leadership for developing and promulgating agency information resource management policies, standards, guidelines, and procedures on data management, system life-cycle management, security, telecommunications, IT reviews, and other related areas. The CIO ensures conformance to these policies.

(4) Provide national leadership for coordination of long-range and strategic planning for information technology investments consistent with departmental initiatives to share data and information at all levels and improve services to customers.

(5) Maintain liaison with the Department, oversight agencies, and other agencies relating to information technology. Prepare related reports and plans requested or required by the Department or oversight agencies. Advise NRCS leadership on information technology actions and policy issues.

(6) Provide leadership in identifying and evaluating new information technologies. Coordinate activities with the Information Technology Division and Information Technology Center to ensure relevance and efficiency in technology recommendations to the agency.

(7) Provide leadership in establishing and maintaining an IT Review Program on major information systems and their management within NRCS. Ensure that the reviews are conducted in compliance with established departmental and external policies, standards, and guidelines.

(8) Designate a responsible individual to serve as NRCS Information Systems Security Program Manager (ISSPM). Ensure that the ISSPM and system administrators work with business project leaders in designing security into the earliest stages of the system development lifecycle. Budget and commit adequate resources for IT security to ensure compliance with all Federal and departmental IT security requirements.

(9) Respond to Congressional and ad-hoc inquiries concerning NRCS programs, budgets or other IT activities.

(c) The Director, Information Technology Center, has the following responsibilities:

(1) Provide technical support to the NRCS CIO in the preparation and submission of A-11 budget reports to the Department, and the coordination of technical approval authorities delegated to the CIO.

(2) Provide leadership in the development, integration, deployment, and support of national software. Provide consultation on gathering business and budget requirements and work with regions and States in local software development efforts and manage the technical approval process.

(3) Support the development and implementation of agency and USDA information technology architectures that support the USDA Service Center environment.

(4) Provide technical support for the creation and operation of the NRCS World Wide Web Home Page and other web-based applications.

(5) Provide technical assistance to the field in support of automated conservation program delivery tools, local and wide area network administration, computer and software engineering technical assistance, and training.

(6) Provide the technical leadership for establishing and maintaining a National Help Desk infrastructure. Ensure that the National Help Desk supports software applications and responds to problems related to hardware, software, telecommunications, security, networking at all organizational units, and supports the Service Center Initiatives, as well as providing assistance to partner agencies personnel.

(7) Provide technical support for operational security.

(8) Perform configuration management, inventory control, and operational support for agency application information systems.

(9) Provide support for telecommunications management for NRCS, including planning, coordinating, and implementing all telecommunications services and equipment.

(10) Provide technical support for Service Center, data management, geographic information system (GIS), telecommunications, and security initiatives.

(11) Provide quality assurance for national information systems, including reviewing, evaluating, testing, and certifying software for national deployment.

(12) Plan, design, coordinate, integrate, test, and maintain approved information systems using commercial off-the-shelf tools and products where feasible.

(13) Identify and evaluate new information technologies. Coordinate activities with the NRCS Chief Information Officer and the Information Technology Division to ensure relevance and efficiency in technology recommendations to the agency.

(14) Develop cooperative projects with other NRCS Institutes and Centers, universities, commercial vendors, technology development centers, experiment stations, and other local, State, and Federal government entities. Products are integrated methodologies, training documents, technology descriptions, code or documented

code segments, technology transfer documents, training sessions and workshops, scientific papers, or other technical documentation.

(15) Initiate, develop, maintain, and support national software and database application projects in accordance with policies and procedures.

(16) Develop software according to approved life cycle methodologies.

Plan, develop, and maintain applications that collect and manage natural resource data, including the National Soil Information System, PLANTS, and other NRCS initiatives.

(d) Deputy Chiefs and Division Directors will:

(1) Designate business area sponsors to work collaboratively with the Information Technology Division and the Information Technology Center as technical and business area specialists in the design and implementation of information systems.

(2) Serve as a member of the Information Resources Management Review Board (IRB).

(3) Initiate, develop, maintain, and support software and database projects in accordance with policies and procedures.

(4) Provide input to the NRCS IT Long-Range Plan and the NRCS IT Manual.

(e) National Headquarters Business Area Sponsors will:

(1) Provide input to the NRCS IT Long-Range Plan and the NRCS IT Manual.

(2) Define software needs by determining user requirements.

(3) Ensure that software development activities meet NRCS business needs.

(4) Establish and maintain an infrastructure that supports custom software, general purpose commercial software, and shared utilities software.

(5) Provide data and information needed in response to requests from the agency and the Department.

(6) Respond to specific software or database systems requests for assistance regarding their systems.

(7) Provide progress reports to the NRCS CIO.

(f) Regional Conservationists will:

(1) Plan, coordinate, manage, and implement all aspects of technical information systems and initiatives of the regional office.

(2) Designate an IT coordinator/administrator to manage and coordinate regional IT support functions to ensure that the installation, operation, and use of the IT system complies with IT policies and procedures.

(3) Designate a local IT security coordinator to ensure that NRCS operations in all offices are in compliance with all Federal policies and procedures.

(4) Designate a security coordinator responsible for conducting an annual security review and developing security plans in accordance with Federal policies.

(5) Provide information technology transfer assistance to States, including training, systems administration, and technical assistance.

(6) Establish a communications channel for sharing IT information.

(g) State Conservationists will:

(1) Plan, coordinate, manage, and implement a comprehensive State IT program. The State Conservationist has overall responsibility and accountability for the information technology activities for area and field offices.

(2) Establish an IT infrastructure to support statewide organizational IT functions in accordance with policies and procedures.

(3) Establish and maintain a technical approval process for procurements within the delegated authority thresholds provided to each State or service center.

(4) Maintain IT support for State and local offices by responding to requests within their State. Identify and train personnel as appropriate.

(5) Designate a security coordinator responsible for conducting an annual security review and developing security plans in accordance with Federal policies.

(h) All Deputy Chiefs, Division Directors, Center Directors, Regional Conservationists, and State Conservationists will:

(1) Manage the IT activities of their area of responsibility in accordance with Federal policies and procedures.

(2) Ensure the security of systems and data.

(3) Initiate, develop, maintain, and support software and database projects in accordance with policies and procedures.

(4) Coordinate IT policy issues with the NRCS CIO.

(5) Provide assistance and a channel for feedback for all State sponsored projects impacting area offices, field offices, and other States.

(6) Provide a vehicle for training of all State-sponsored IT projects which impact area offices, field offices, and other States.

(7) Ensure that documentation, maintenance and support of State developed software is performed.

(i) All NRCS employees, volunteers, contractors, or any person using, managing, operating, supporting or involved with the acquisition, implementation, and/or upgrade of NRCS equipment are responsible and accountable for the following:

(1) Perform all IT-related activities in accordance with departmental and agency policies and procedures.

(2) Secure and manage IT equipment by backing up files, ensuring backups offsite, encrypting sensitive data, and using password protection on all workstations.

(3) Participate in mandatory periodic training in computer security awareness and accepted practices involved in the management, use, or operation of Federal computer systems.

(4) Follow policy that defines use by employees on government telephone systems in accordance with departmental and agency policy.

(5) Utilize the USDA Internet, World Wide Web (WWW), and E-mail to perform NRCS official business or limited personal use in accordance with departmental and agency policy. E-mail shall not contain discriminatory language or contain remarks that constitute sexual harassment.

(6) Exercise all precautions to prevent infecting systems by downloading files from the Internet, E-mails, CDs or diskettes that contain viruses, Trojan horses, or other 'exe' attachments.

(7) Use facsimile machine for official documents that are time sensitive or that require an immediate response. Sensitive information should not be transmitted via fax.

The following table is a summary of organizational units with lead responsibility for IT functions and activities in NRCS.

Table 501.1 Information Technology Roles and Responsibilities

	Lead Responsibility		
Function	**Information Technology Division (ITD)**	**Information Technology Center (ITC)**	**National Cartographic & Geospatial Center (NCGC)**
Budgeting - A-11 Report	X		
Configuration Management		X	
Data Acquisition			X
Data Administration	X		
Data Delivery			X
Data Integration			X
Data Quality			X

	Lead Responsibility		
Function	**Information Technology Division (ITD)**	**Information Technology Center (ITC)**	**National Cartographic & Geospatial Center (NCGC)**
Data Warehousing			X
Departmental Computer Centers	X		
Electronic Equipment Accessibility		X	
GIS	X	X	X
Hardware Testing and Integration		X	
Help Desk		X	
Internet		X	
IT Future Technology/Research		X	
National Policy Development	X		
Reviews	X		
Security	X	X	
Software Development		X	
Software Testing, Certification, and Distribution		X	
Strategic and Long-Range Planning	X		
Technical Approval		X	
?? **Technical Assistance**	??	?? X	??

	Lead Responsibility		
Function	**Information Technology Division (ITD)**	**Information Technology Center (ITC)**	**National Cartographic & Geospatial Center (NCGC)**
?? **Computers** ?? **Software Engineering**			
Telecommunications		X	
Training, Delivery		X	
Training, Development		X	
Waivers	X		

SUBPART B - BOARDS AND COMMITTEES

501.10 Purpose.

501.11 Authorities.

501.12 Policy.

501.13 Responsibilities.

PART 501 - IRM ORGANIZATIONS: ROLES AND RESPONSIBILITIES

SUBPART B - BOARDS AND COMMITTEES

501.10 Purpose.

To describe the overall IRM policy, management, and oversight responsibilities of departmental and agency boards, committees, and consortiums.

501.11 Authorities.

(a) Clinger-Cohen Act of 1996, Public Law 104-106.

(b) USDA Executive Information Technology Investment Review Board Charter, March 1997.

(c) USDA Information Resources Council Board Charter.

(d) NRCS Information Resources Management Review Board Charter, October 1996.

(e) USDA IRM Modernization Project Report, November 1995.

(f) Government Paperwork Elimination Act (GPEA), Public Law 105-277, October 1998.

501.12 Policy.

(a) NRCS will actively support and participate in departmental and NRCS boards, committees, and consortiums.

(b) NRCS will adhere to decisions and recommendations set forth by the governing and oversight boards.

501.13 Responsibilities.

(a) USDA Executive Information Technology Investment Review Board (EITIRB) is comprised of departmental senior-level managers to ensure USDA technology investments are managed as strategic business resources supporting efficient and effective program delivery.

The EITIRB will:

(1) Evaluate existing projects, operational systems, department-wide IT initiatives, and approve new information technology investments to create a USDA information technology investment portfolio.

(2) Use a standard set of criteria to assemble the USDA investment portfolio and to evaluate agency and department-wide IT initiatives. The criteria include departmental or government-wide impact, visibility, cost, risk, architecture, and standards.

(3) Provide a critical link between the program, business, and IRM organizations at the highest level.

(b) The USDA IT Leadership Council members are the USDA Chief Information Officer and senior IT officials for each USDA mission area. The Council is accountable to the USDA Chief Information Officer and will:

(1) Be accountable for information technology planning, budgeting, and policy decisions of USDA-wide IT initiatives.

(2) Serve as a resource for IT issues on a Department-wide basis and respond with strategies and policies for the development and deployment of solutions that address USDA's corporate interests.

(3) Ensure coordination and integration of activities to avoid duplication of effort.

(4) Establish sub-councils and ad-hoc teams to support new IT initiatives as well as ongoing projects having significant Department-wide impact.

(c) NRCS Information Resources Management Review Board (IRB) members are NRCS Deputy Chiefs, a representative of the National Association of State Conservation Agencies (Ex Officio), a representative of the National Association of Conservation Districts (Ex Officio), and the NRCS Chief Information Officer. IRB is accountable to the NRCS Chief and will:

(1) Carry out responsibilities assigned by various legislative Acts, e.g., Clinger-Cohen Act of 1998, Public Law 104-106.

(2) Review and approve plans and budgets of proposed major information resources management projects or systems at initiation and at major milestone during implementation.

(3) Establish system development priorities based on business strategic plans.

(4) Develop and prioritize the agency IT annual budget for all agency-wide information technology and information resources investments and expenditures.

(5) Provide agency oversight and accountability for agency IT functions.

(6) Review and approve the agency's IT Long-Range Plan, including IT procurements.

(7) Evaluate the performance of all major information systems.

(8) Ensure that the agency's IT activities are integrated and compatible and support partners' information systems and needs.

(d) The Management Services Division's Information Technology Acquisition Team (ITAT) establishes and manages contracts for outside services; maintains a contract file for all deliverables specified in contracts; and provides the Contract Officer for all contracts. The ITAT team will:

(1) Provide a full range of IT acquisitions nationwide for NRCS and partnering agencies within USDA and other USDA agencies.

(2) Provide assistance to special projects sponsored by USDA's Procurement Policy Division, such as the Procurement Modernization Team (PMT).

(3) Establish and maintain procedures to be utilized by NRCS to procure IT resources, and establish procedures to be used by Government-Wide Agency Contracts (GWACs).

PART 502 - SECURITY MANAGEMENT

SUBPART A – GENERAL

PART 502 – SECURITY MANAGEMENT

SUBPART A - GENERAL

502.0 General.

To provide policy, guidelines, and responsibilities for safeguarding and securing NRCS Information Technology (IT) resources.

502.1 Policy.

(a) NRCS will maintain a comprehensive and effective security program that adequately protects IT resources. This program complies with all Federal and departmental standards, regulations, and laws in the area of IT security.

(b) The agency security functions are delegated to the CIO, Information Technology Division. Stated security policies, procedures, and responsibilities apply to the entire agency.

(c) The agency will supplement the USDA ADP Security Manual, DM 3140-1, when appropriate, with national and State supplements.

502.2 Authorities.

(a) Computer Security Act of 1987, Public Law 100-235.

(b) Freedom of Information Act (FOIA) of 1980, Public Law 93-502.

(c) Privacy Act of 1974, 5 U.S.C. 552a.

(d) Network Protocol Analyzers, Departmental Note (DN) 3140-9.

(e) Implementation of Gateway and Firewall Policy and Technical Security Standards, DN 3140-6.

(f) Implementation of Securing Sensitive Information on Servers, DN 3140-8.

(g) Security Requirements for Government Employees, Executive Order Number 10450, April 1953.

(h) Security of Federal Automated Information Systems, Appendix III, Office of Management and Budget (OMB) Circular Number A-130, February 1996.

(i) USDA Automated Data Processing (ADP) Security Manual, Departmental Manual (DM) Number 3140-1, July 1984.

(j) USDA Information Systems Security Policy, May 1996.

(l) USDA Internet Security Policy, March 1995.

(m) Information Security Reform Act of 2000, PL 106-398.

(n) Telecommunications and Internet Services and Use, USDA Departmental Regulation (DR) 3300-002, March 1999.

(o) Presidential Decision Directive 63: Critical infrastructure Protection, May 1998.

(p) OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Systems, July 1998.

(q) Department of Defense Trusted Computer System Evaluation Criteria, 5200.28-STD, December 1985.

502.3 Definitions.

(a) Departmental Computer Centers (DCCs). The National Information Technology Center (NITC) at Kansas City, Missouri, as well as the National Finance Center (NFC) in New Orleans, Louisiana, are DCCs. The DCCs are vital and major sources of computer services and related activities, as designated by the Secretary of the U. S. Department of Agriculture.

(b) DCC Access. The process of properly accessing a Departmental Computer Center. This includes the proper establishment of DCC logon ID's, passwords, and remote ID's and security clearances.

(c) Computer System. One or more computers and attached peripherals that may be connected by a telecommunications network.

(d) Federal Computer System. The Computer Security Act of 1987 defines a "Federal computer system" as a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function.

(e) Sensitive Data. Information which loss, unauthorized modification, or unauthorized disclosure would be detrimental to agency operations. It includes information that is personal (requiring protection under the Privacy Act), proprietary, or critical to agency plans and operations. Sensitive data is also classified in the national security or associated with fiduciary or financial transactions.

(f) Types of Information Technology Facilities:

(1) Type I Information Technology (IT) Facilities. Departmental Computer Centers.

(2) Type II Information Technology (IT) Facilities. State offices, regional offices, large centers, and National Headquarters offices are considered Type II facilities.

(3) Type III Information Technology (IT) Facilities. Area and field service centers are considered Type III facilities.

(4) Low-activity Office Environments. Offices which have three (3) or less user logon IDs on the local IT multi-user system.

502.4 Responsibilities.

(a) The NRCS Chief Information Officer (CIO) has the following responsibilities:

(1) Determine the NRCS mission requirements for IT security and for furnishing adequate personal data, as defined in the Privacy Act of 1974, and other sensitive data.

(2) Establish an agency-wide program for IT security, consistent with the mission of the agency.

(3) Designate a responsible individual to serve as the agency IT Information Systems Security Program Manager (ISSPM).

(4) Ensure that the ISSPM and system administrators work with business project leaders in designing security into the earliest stages of the system development lifecycle.

(5) Budget and commit adequate resources for IT security to ensure compliance with all Federal and departmental IT security requirements.

(b) The NRCS Information Systems Security Program Manager (ISSPM) has the following responsibilities:

(1) Provide management and oversight of the NRCS Security Program.

(2) Advise management of security policies and procedures.

(3) Assist and advise local IT security coordinators in IT security program development and administration.

(4) Review applicable technical approval (TA) requests to assess and certify the sensitivity of proposed requests, where applicable.

(5) Coordinate the development and documentation of a national set of system administration security utilities for use on all office multi-user machines.

(6) Identify additional security controls that are necessary to minimize security risks and potential loss.

(7) Review all security incidents and corrective actions taken at any NRCS location and ensure that corrective action takes place.

(8) Ensure that all computer systems security requirements meet NRCS requirements.

(9) Develop a security awareness training program that addresses common security problems and concerns.

(10) Develop internal security standards and procedures for all levels of employees.

(11) Keep abreast of security regulation and law updates and changes.

(12) Serve as liaison to interagency project managers for the security components of these projects. Projects include LAN/WAN/Voice (LWV), Combined Administrative Management System (CAMS), Service Center Initiatives for Business Process Reengineering (BPR), Electronic Access Initiative (EAI), and Common Computing Environment (CCE). This will include reviewing the security architecture for these projects. Update and review Interoperability Lab (IOL) security rules for the CCE equipment used by NRCS employees.

(13) Participate in Departmental security initiatives such as encryption, PKI, digital certificate, intrusion detection, anti-virus protection, monitoring tools, firewalls, routers, disaster recovery, and risk assessments, and identify appropriate policy.

(c) The NRCS Deputy Information Systems Security Program Managers (Deputy ISSPMs) have the following responsibilities:

(1) Assist local IT Departmental Computer Center (DCC) Access Coordinators with DCC access requirements.

(2) Provide oversight for security plan development for general support systems and major application development.

(3) Assist ISSPM with the management of the NRCS security program.

(4) Update the National Information Security Handbook as needed.

(d) State Conservationists, Regional Conservationists, and Deputy Chiefs have the following responsibilities:

(1) Designate a local IT security coordinator to ensure that NRCS operations in all offices are in compliance with the USDA Departmental Security Manual and all corresponding agency policy.

(2) Designate a local DCC access coordinator and a backup DCC access coordinator for all DCC access needs.

(3) Designate an IT system administrator for each IT system to ensure that the installation, operation, and use of the IT system complies with IT policies and procedures.

(4) Ensure that steps are taken to maintain security risks at an acceptable level.

502.5 Performance Work Plans.

All employees with direct responsibility for information systems security will have a security performance element in their Performance Work Plan, SCA Form 4140. The element will be commensurate with the level of responsibility the employee has for security. Employees in the following positions are required to have a security element:

(a) The NRCS Chief Information Officer and his/her direct reports.

(b) The NRCS Information Systems Security Program Manager (ISSPM) and his/her direct reports.

(c) The NRCS Information System Security Program Deputy Manager and his/her direct reports.

(d) Those employees designated by the ISSPM as having a level of information systems security responsibility requiring a security performance element.

SUBPART B - USE OF IT SYSTEMS

502.10 Purpose.

502.11 Policy.

502.12 Definitions.

502.13 Application Systems and Files.

502.14 Securing IT Equipment.

502.15 DCC Access.

502.16 Security Awareness Training.

502.17 Security Clearances.

502.18 Security Clearances for Contractors.

502.19 Security Clearance Exit Interview.

PART 502 – SECURITY MANAGEMENT

SUBPART B – USE OF IT SYSTEMS

502.10 Purpose.

This subpart contains policy and guidance on security training, system access, and security clearances.

502.11 Policy.

(a) All system logon ids will have a password. Factory installed default passwords for workstations, routers, firewalls, web servers, and other network hardware devices and software servers will be changed. User ids and logon ids are for one person only and will not be shared.

(b) Users of CCE equipment must follow the guidelines that are set in the CCE Systems Administrators Guide and the CCE Users Guide for password protection and security protection of the system.

(c) Passwords are issued to protect and control systems access. All IT system administrators will enforce the use of passwords on IT multi-user systems. Passwords are for one person only and will not be shared with other individuals.

(d) Single-user systems containing sensitive information will either be protected with a password or locking capability (preferably both).

(e) For all systems, the local IT security coordinator will develop a standby back-up plan, in accordance with OMB Circular A-130. Refer to the specific security plan for each major application and general support system for the back-up frequency and procedures.

(f) All IT systems will be backed up on a regular basis. Periodic backups must be stored at a secure off-site location designed to protect them from theft and disasters.

(g) NRCS systems with information designated as sensitive to unauthorized disclosure will have additional security controls based on benefit/cost analysis, as specified in OMB Circular A-130. Information is sensitive to unauthorized disclosure if it contains information that is covered by the Privacy Act of 1974 or is exempt from disclosure under the Freedom of Information Act.

(h) Federal employees, contractors, and non-Federal employees using any NRCS system will have security clearances as outlined in Table 502.1.

(i) National Headquarters and Service Center offices, which have received CCE computers and software, must follow guidelines set up by the Interoperability Lab (IOL). These

guidelines are defined in the CCE System Administrators Guide and CCE Users Guide. Restrictions are set on these machines to prevent disability virus software or changing security or password rules.

(j) Network Scanning and Monitoring

(1) DN 3140-9 requires that all network scanning and monitoring devices and operators must be registered with the USDA Office of Cyber Security. Further, it requires operators of such hardware and software are to be properly trained and certified.

(2) All NRCS organizational units having network scanning and monitoring devices will register them with the Department and provide this registration information to the NRCS Chief Information Officer and NRCS Information System Security Program Manager.

(3) Any NRCS organizational unit that plans to use network scanning or monitoring devices for other than analysis of network operations shall have the written consent of the Deputy Chief for Management. Delegation of this responsibility is not permitted. Prior to the beginning of scanning or monitoring, the NRCS Chief Information Officer and the NRCS ISSPM shall be notified of the proposed start date, duration, scope, and purpose of the scanning or monitoring.

(4) The NRCS CIO or Information System Security Program Manager is available for assistance and consultation on matters relating to network scanning and monitoring.

502.12 Definitions.

(a) Network scanning and monitoring. Scanning and monitoring as used in this part refer to the scanning or monitoring of network activities; e.g., sniffers, network analyzers, whether software or hardware.

(b) Vulnerable to service interruptions. A system is considered vulnerable to service interruptions if there would be a substantial cost for standby measures to provide for timely resumption of processing following a service interruption. Standby costs include maintaining additional hardware, fees for the right to access a commercial backup facility, and the costs of administering an agreement for a mutual backup plan. These costs exclude the fees for maintaining off-site backup.

(c) Vulnerable to fraud. A system is considered vulnerable to fraud if it is possible to circumvent data controls to alter the software or data files so as to affect or conceal a fraud or delay its detection.

502.13 Application Systems and Files.

All NRCS application systems and related data must have security plans demonstrating adequate controls when unauthorized use of said systems or data results in:

(a) Fraud, theft, or illegal gains from automated programs that issue payments, benefits, receipts, or billings;

(b) Miscalculation of payments, benefits, receipts, billings, or inventories;

(c) Fraud, theft, or illegal gains from automated programs that maintain inventories;

(d) An adverse effect on agency investigations, operations, or the production of time-critical data from used or altered files; or

(e) A breach of national defense security or in the loss of life from unauthorized disclosure or alterations to files.

502.14 Securing IT Equipment.

All NRCS employees are responsible for security related to physical access, including access for visitors, procedures for office opening and closing, knowledge of fire safety procedures, use of burglar alarms, proper storage of IT equipment, and the care of equipment, including the use of laptop computers. NRCS personnel must follow rules set by NRCS and CCE security plans.

502.15 DCC Access.

The supervisor or employee must direct all DCC access requests to the local IT DCC access coordinator.

502.16 Security Awareness Training.

(a) The Computer Security Act of 1987 requires mandatory yearly training in computer security awareness and accepted practices for all employees involved in the management, use, or operation of Federal computer systems.

(b) NRCS policy is to support security training as outlined by the National Institute of Standards and Technology Special Publication Information Technology Security Requirements: A Role and Performance-Based Model (NIST Special Publication 800-16).

502.17 Security Clearances.

(a) NRCS will have the following security clearances performed on employees:*

(1) National Agency Check with Law and Credit (NACLC).

(2) Limited Background Investigation (LBI).

(3) Background Investigation (BI).

* Please refer to Table 502.1 for clarification of what clearance each employee needs.

(b) Security clearances are the responsibility of the NRCS ISSPM and Deputy ISSPMs for National Headquarters. They are also responsible for ensuring that security personnel in each State and service center have the necessary security clearances.

(c) Background investigations and security clearances will be conducted on employees commensurate with their position sensitivity, level of access, and need to know. At the minimum, all employees will be subject to a National Agency Check with Law and Credit (NACLC) check. Employees include both permanent and temporary NRCS employees, contractors, and personnel accessing NRCS computer systems with the privileges that would be afforded an NRCS employee performing in the same position. This latter category would include volunteers and employees of NRCS partners such as conservation districts and other State and local agencies. Table 502.1 lists security clearance levels for various employee categories.

Table 502.1 Security Clearance Levels

Personnel	Security Clearance Level	Periodicity (years)
All Employees (including IT personnel not listed below)	National Agency Check with Law and Credit (NACLC).	10
Non-supervisory System Administrators	Limited Background Investigation (LBI).	5
Supervisory System Administrators	Background Investigation (BI).	5
Program Managers	Limited Background Investigation (LBI).	5
Technical Help Desk Personnel	Limited Background Investigation (LBI).	5
Program Help Desk Personnel	National Agency Check with Law and Credit (NACLC).	10
Security Staff and State Security Officers	Background Investigation (BI).	5
Financial Personnel (05XX series)	National Agency Check with Law and Credit (NACLC).	5
Personnel Staff	National Agency Check with Law and Credit (NACLC)	5

	Law and Credit (NACLC).	
Contracting Officers	National Agency Check with Law and Credit (NACLC).	5

(d) When a higher level of access is needed to meet operational or contractual exigencies not expected to be of a recurring nature; will not exceed 180 days; and is limited to specific, identifiable information, temporary access may be granted by security personnel authorized by the agency.

(e) Individuals whose job, scope of responsibilities, levels of access, and/or duties significantly change so that their initial investigation is insufficient to support the incumbents' current needs require an updated, upgraded reinvestigation within 120 days of reassignment, promotion, or reclassification.

(f) A periodic reinvestigation, dependent on the original level of investigation or clearance, is required and will be conducted. All NACLC clearances, except for contracting officers, and financial and personnel specialists, will be reinvestigated every 10 years. All BI, LB, and NACLC clearances for contracting officers and financial and personnel specialists require reinvestigations every 5 years.

(g) All accesses will be contingent upon favorable investigations or periodic reinvestigations. Incumbents who occupy positions that require favorable background investigations, and whose investigations are returned unfavorable, will have *all* accesses suspended or revoked until such time that the individual can address the deficiencies and successfully undergo a favorable investigation.

502.18 Security Clearances for Contractors.

At the minimum, contractors will have a National Agency Check with Law and Credit (NACLC) before having access to any systems granted them. Additional investigations, or clearances, are required commensurate with their position sensitivity, level of access, and need to know. These investigations will be the responsibility of the contractor and will be incorporated in the Federal contract. Contractors performing system administration functions require BI clearances.

502.19 Security Clearance Exit Interview.

(a) When an IT security clearance is no longer required for an employee, the employee must complete a security clearance exit interview form (SF-312). Instances where an employee may no longer require a security clearance include a change in job functions, termination, or resignation.

(b) The local IT security coordinator, IT system administrator or supervisor is responsible for witnessing the signing of the security clearance exit interview form.

(c) The employee's supervisor is responsible for ensuring that a copy of the security clearance exit interview form is filed in the employee's Official Personnel Folder.

SUBPART C - SECURITY REVIEW AND REPORTING

502.20 Purpose.

502.21 Risk Assessment.

502.22 Responsibilities.

502.23 Annual Security Review.

502.24 Site Security Plan.

502.25 System Security Plan.

502.26 Trusted Facilities Manual.

502.27 Business Continuity Plan (BCP) (formerly DisastRecovery Plan).

502.28 Theft or Property Damage.

502.29 Security Violations.

PART 502 – SECURITY MANAGEMENT

SUBPART C - SECURITY REVIEW AND REPORTING

502.20 Purpose.

Guidance and responsibilities in the areas of security reviews, reporting, and risk assessments are included in this subpart.

502.21 Risk Assessment.

NRCS bases its IT security program on a quantitative and/or a qualitative analysis of risks and threats, a risk assessment. Security measures are recommended according to assessed risks. Major factors in a risk assessment include the value of systems or applications, threats, vulnerabilities, or the effectiveness of current safeguards. The risk assessment is intended as a management tool for making decisions on the use of resources.

502.22 Responsibilities.

(a) The ISSPM will provide leadership in developing and maintaining a formal risk assessment for all agency application information systems (AISs) in collaboration with the appropriate business sponsors.

(b) Annually in March, the ISSPM and Deputy ISSPMs will review each AIS risk assessment for any material changes in the data or assumptions. Changes will be reported to the Department in April of the same year.

(c) A risk assessment must be performed at intervals of three (3) years or when hardware, system software, or the office environment is significantly modified. The risk assessment must identify physical security risks as well as information technology (IT) risks.

502.23 Annual Security Review.

(a) DM 3140-1 requires all Type II and Type III facilities to perform an annual security review. A security review consists of an evaluation of physical security, operating procedures, and personnel practices as outlined in the site security plan. It consists of an evaluation of physical security, operating procedures, and personnel practices. Generally, identified vulnerabilities can be countered by relatively simple and inexpensive measures. Potentially serious security problems that are identified during a security review must be addressed immediately.

(b) The local IT security coordinators are responsible for performing annual security reviews in designated State and regional offices.

(c) The IT system administrators in area and field offices are responsible for the annual security review.

(d) Appropriate measures must be taken to correct deficiencies identified during the review. The annual security review is an accountable item in an IRM appraisal.

(e) Offices are responsible for completing annual reviews no later than February 15. The review document must be maintained on file at the location of the review until a subsequent review is completed. Information and formats for the plan can be found in the Security Handbook.

502.24 Site Security Plan.

(a) All offices must develop a site security plan as outlined in the USDA Departmental Manual, DM 3140-1, Management of ADP Security Manual. State offices, regional offices, National Headquarters office, centers and institutes will forward a copy of the site security plan to the NRCS ISSPM. NRCS field offices will forward the site security plan to the appropriate State office.

(b) The site security plan will be retained on file. It will be reviewed and updated annually.

(c) All security plans will contain business continuity measures, in accordance with the guidance in the USDA ADP Security Manual, DM 3140-1.

(d) All employees will be informed in the event of significant changes to the existing Site Security Plan.

502.25 System Security Plan.

(a) Additional security plans will be developed for General Support Systems and major AISs. Sponsors of major AISs will develop a security plan and risk assessment as necessary for that specific plan.

(b) Applications or General Support Systems under development will contain a security statement describing the project requirements for security and the planned method for implementation. This statement will be valid for a period not to exceed the first year of development, at which time a secondary statement will be required.

502.26 Trusted Facilities Manual.

A trusted facilities manual will be developed for General Support Systems describing how to configure and install a specific secure system, how to operate in a secure manner, and describe the effective use of system privileges and protection mechanisms.

502.27 Business Continuity Plan (BCP) *(formerly Disaster Recovery Plan).*

All offices must have a Business Continuity Plan (BCP) to protect agency and IT facilities against unacceptable loss. The BCP can be a component of the site security plan. The BCP must be maintained and followed in the event of an emergency or disaster and address, at a minimum, the following areas:

(a) Maintaining adequate materials at the back-up site, including current programs, data, documentation, and supplies;

(b) Handling of the emergency (fire-fighting, building evacuation procedures, power outages, etc.); and

(c) Moving people, data, and support to an alternate site(s).

502.28 Theft or Property Damage.

(a) User Responsibility. All employees are responsible for immediately reporting all incidents of theft or damage to IT hardware or software, or any suspicion of fraud, tampering, or unauthorized disclosure of data to the local IT security coordinator and to the supervisor. The local IT security coordinator or IT system administrator is responsible for notifying the next level security coordinator and the NRCS ISSPM.

(b) Accountable Property Officer Responsibility. The accountable property officer is responsible for working with the employee to complete Form AD-112, Report of Unserviceable, Lost, or Damaged Property, in accordance with NRCS General Manual 120-405.44.

502.29 Security Violations.

(a) The local IT security coordinator or IT system administrator must report to the NRCS ISSPM, through administrative channels, any incident involving:

(1) Suspected fraud involving an IT system or unauthorized disclosure of sensitive data.

(2) Suspected cases of significant personal use of IT systems.

(3) Attempted or actual unauthorized access (logging on) to a Federal computer system.

(4) Security breaches involving root or administrator compromise of systems or breaches involving the modification of web servers or web pages.

(b) If a security breach occurs:

(1) IT security coordinators must report in writing to the NRCS ISSPM security breaches that involve root or administrator compromise or modification of web sites.

This report should include the nature and extent of the breach, how the breach was discovered, how the breach was resolved, and copies of the portions of the system log files that document the incident.

(3) System administrators will immediately disconnect the breached system from the network, save the appropriate system log files for investigation, repair the system from a "clean" back-up, or rebuild the system from the original system software. Backups of breached systems shall be kept under proper chain of custody and held under lock and key until transferred to proper authority.

(4) The violation must also be reported to the local personnel officer responsible for the security of sensitive personnel files, if sensitive data, (e.g., name of employee, social security number), has been compromised as a result of the breach.

SUBPART D - DEPARTMENTAL COMPUTER CENTER ACCESS

502.30 Purpose.

502.31 Policy.

502.32 Responsibilities.

PART 502 – SECURITY MANAGEMENT

SUBPART D - DEPARTMENTAL COMPUTER CENTER ACCESS

502.30 Purpose.

This part provides policy and responsibilities for using the Departmental Computer Centers (DCC).

502.31 Policy.

The Departmental Computer Centers (DCC's) must be the first source of supply for all IT mainframe operational services. A waiver of this policy must be obtained prior to selecting and using any other facility.

502.32 Responsibilities.

(a) All offices are responsible for ensuring that criteria for waivers of IRM policy and security have been met before and during use of DCCs as well as with other approved sources of computer services. Please refer to part 504 - Information Technology Technical Approval (TA) for supplementary information.

(b) The DCC is responsible for establishing policies and procedures to manage access by users. The ISSPM and Deputy ISSPMs are responsible for implementing the policy.

(c) National project managers are responsible for preparing a DCC Impact Statement.

(d) Users are responsible for contacting their local DCC Access Coordinator to obtain access to DCC facilities.

(e) Except where otherwise noted, DCC Access Coordinators will contact the National Help Desk for all DCC access requests, including the establishment of new users, changes in user privileges, and remote printer ids.

(f) Certain major applications (e.g., CAMS, EARN, PCMS) access Departmental Computer Centers. However, the establishment and management of user access to the DCCs are managed by the major application owners. DCC Access Coordinators should contact the appropriate designated official for these applications.

(g) The NRCS DCC Access Coordinators need to notify the NRCS national security staff of all employee separations for the immediate deletion or suspension of affected user ids.

PART 503 - IRM PLANNING AND CAPITAL INVESTMENTS

SUBPART A - IRM PLANNING

PART 503 - IRM PLANNING AND CAPITAL INVESTMENTS

SUBPART A - IRM PLANNING

503.0 Purpose.

To establish guidelines and responsibilities for the IRM strategic planning process within the organizational components of NRCS.

503.1 Authorities.

(a) Chief Financial Officers Act (CFO Act).

(b) Government Performance and Results Act (GPRA) of 1993, Public Law 103-62.

(c) Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995.

(d) Clinger-Cohen Act of 1996, Public Law 104-106.

(e) Federal Acquisition Streamlining Act (FASA).

(f) Management Accountability and Control, Office of Management and Budget (OMB) Circular A-123.

(g) Departmental Long-Range IRM Planning, USDA Departmental Regulation (DR) 3111-001, February 1989.

(h) USDA Guide to Information Technology Capitol Planning, Draft USDA Publication, updated annually.

(i) Plan of Operations, NRCS General Manual (GM) 330-401.3.

(j) Policy on Oversight and Evaluation, NRCS General Manual (GM) 330-405, 9/23/96.

(k) Principles of Budgeting for Capital Asset Acquisitions, Office of Management and Budget Publication, 1997.

(l) USDA Information Systems Technology Architecture, February 1997.

(m) USDA IRM Strategic Plan.

503.2 Policy.

(a) NRCS will produce an annual IRM Strategic Five-year Long-Range Plan for submission to the Department. The IT planning efforts described in the plan will comply with the annual USDA planning guidance, approved USDA and NRCS information systems technology architectures. IT planning efforts will also meet USDA and Federal Capital Planning principles.

(b) Business area leaders will communicate their requirements to the Chief Information Officer in a timely fashion. This communication will help to facilitate the planning of software development to meet changing short-term business area requirements.

503.3 Definitions.

(a) Application Information System (AIS). The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures as part of one or more business processes. It includes hardware, software, personnel, telecommunications services, support services, and intra-governmental services.

(b) IT Performance Plan. An annual plan describing performance measures, goals, and outcomes associated with each major application information system. The performance plan, based on the Clinger-Cohen Act and the IT Strategic Long-Range Plan, will cover a one-year period and tie IT initiatives to the NRCS GPRA goals and outcomes they support.

(c) IT Strategic Long-Range Plan. A five-year plan developed according to departmental guidelines that describes NRCS' Information Technology management program, structure, approval processes, and planned major initiatives that support the business goals of the agency.

(d) Information Systems Technology Architecture (ISTA). The ISTA provides a blueprint for information technology hardware, software, telecommunications, data, and security standards, based on agency core business processes and associated information. The intent of ISTA is to ensure that agency and department IT plans and acquisitions meet business process needs. It is intended also to facilitate the sharing of information with internal and external Federal agencies, conservation partners, and private organizations.

(e) IT Investment. ITS investment is an expenditure of money and/or resources for IT or IT-related products and serves involving managerial, technical, and organizational risk for which there are expected benefits to the organization's performance. These benefits are defined as improvements either in efficiency of operations or effectiveness in services.

503.4 Responsibilities.

(a) The NRCS Chief Information Officer will:

(1) Develop and submit the NRCS IRM Strategic Plan to the Department's Office of the Chief Information Officer (OCIO).

(2) Incorporate input and data from agency-wide sources into the NRCS IRM Strategic Plan as appropriate.

(3) Coordinate IRM strategic planning efforts with NRCS agency strategic planners and business area sponsors to ensure that IRM planning efforts support the mission, objectives, and outcomes of the agency strategic plan.

(4) Ensure that IRM strategic planning efforts are in compliance with the USDA annual planning guidance, USDA IRM Strategic Plan, and USDA Information Systems Technology Architecture.

(5) Coordinate with partner agencies to ensure that crosscutting and/or interagency initiatives are addressed in the strategic plan.

(6) Coordinate strategic IRM plans with reports to the Department on planned information technology investments.

(7) Develop an Information Technology Performance Plan.

(8) Distribute copies of the annual NRCS IRM Strategic Plan to States, Regions, NHQ Divisions and Offices, Centers, and Institutes.

(b) Center Directors, Institute Directors, and Heads of organization units (except for NHQ Divisions) will:

(1) Produce a plan during each annual planning cycle that describes planned IT acquisitions during the current fiscal year and the following five (5) years. IT acquisitions include hardware, software, data, support services, maintenance services, and interagency or university IT services. Managers will provide information on the number and type of acquisition and the cost of each type of acquisition in each year.

(2) Submit their office IRM Plan to the Information Technology Division annually by May 30.

(c) NHQ Division Directors will:

(1) Sponsor and develop documentation for national application information systems and projects proposed for approval by the Information Resources Management Review Board (IRB). The documentation will include requirements analyses, design and development proposals, benefit-cost analyses, project plans, and performance plans.

(2) Develop project slate information to support the development of the IRM strategic long-range plan and the budget process.

(3) Submit the project documentation approved by the IRB to the Information Technology Division.

(d) Regional Conservationists will:

(1) Consolidate State IRM Plans into a Regional IRM Plan and supplement that plan to reflect the plans and needs of all offices in the region, including the Regional Office, during the current year and the following five (5) years.

(2) Submit their Regional IRM Plans to the NHQ Information Technology Division annually by May 30.

(e) State Conservationists will:

(1) Produce, during each annual planning cycle, plans that describe IT acquisitions planned during the current fiscal year and the following five (5) years. IT acquisitions include hardware, software, data, support services, maintenance services, and interagency or university IT services. State Conservationists will provide information on the number and type of acquisitions and the cost of each type of acquisition within in each year.

(2) Submit IT plans to their Regional Offices annually by April 15.

SUBPART B - INFORMATION TECHNOLOGY SYSTEMS (ITS) REPORT

503.10 Purpose.

503.11 Authorities

503.12 Policy.

503.13 Definitions.

503.14 Responsibilities.

PART 503 - IRM PLANNING AND CAPITAL INVESTMENTS

SUBPART B - INFORMATION TECHNOLOGY SYSTEMS (ITS) REPORT

503.10 Purpose.

To provide policy and responsibilities for collecting and submitting the NRCS information technology (IT) budget estimates.

503.11 Authorities

(a) Planning, Budget, and Acquisition of Capital Assets., Office of Management and Budget (OMB) Circular A-ll.

(b) Management of Federal Information Resources, OMB Circular A-130.

(c) GAO Guide "Information Technology Investment Evaluation Guide". Assessing Risk and Returns: A Guide for Evaluating Federal Agencies ITS Investment Decision-making.

(d) NRCS IRM Strategic Long-Range Plan.

(e) Funding Information Systems Investments, OMB Memorandum M-97-02, October 1996 (also known as "Raines Rules").

(f) USDA Office of the Chief Information Officer (OCIO) Annual Budget Guidance.

503.12 Policy.

NRCS will submit to the Department's OCIO required reports on planned and actual spending for the acquisition, operation, and use of IT systems and facilities in accordance with the provisions of OMB Circular A-11.

503.13 Definitions.

(a) Capital Planning. Capital planning is a systematic approach to managing the risks and returns of IT investments for a given mission area.

(b) Information Technology Systems (ITS) Report. OMB Circular A-11 requires that all departments submit annual reports (ITS reports) on the acquisition, operation, and use of Federal Information Processing (FIP) systems and facilities. The ITS report allows the Department, OMB, and Congress to anticipate requirements for new or continuing IT activities being carried out, including those for which additional funding may be required.

The NRCS CIO submits this report to the Department's OCIO in the spring, fall, and winter of each year.

503.14 Responsibilities.

(a) Regional Conservationists, NHQ Division Directors, Center Directors, and Institute Directors will:

(1) Provide the IT Division with projected cost estimates related to the acquisition, operation, and use of FIP systems and facilities. This information is in the IT plans and project documentation submitted to the ITD each year, as described in subpart A of this section.

(2) Provide additional information regarding IT expenditures or spending plans upon request from the ITD or ITC.

(b) The NRCS Chief Information Officer will:

(1) Share IT cost information and project documentation submitted as part of the planning process with the IT Center for use in compiling ITS investment reports. This coordination will ensure that decision rationale is based on business case criteria and risk is effectively managed and the rate of return is maximized.

(2) Compile projected and actual IT cost data, and benefit-cost analyses for major projects, into the NRCS ITS Report for submission to the OCIO.

(3) Utilize IT resources to obtain data necessary for the ITS report. Resources include ITD, ITC, project managers of major initiatives, the annual Project Slate funding plan and the annual NRCS IT plan.

(4) Coordinate ITS reports with the NHQ Budget Planning and Analysis Division to ensure consistency with agency budget plans and strategies.

PART 504 - INFORMATION TECHNOLOGY TECHNICAL APPROVAL (TA)

504.0 Purpose.

504.1 Authorities.

504.2 Policy.

504.3 Definitions.

504.4 Responsibilities.

PART 504 - INFORMATION TECHNOLOGY TECHNICAL APPROVAL (TA)

504.0 Purpose.

To establish the policy for managing technical approvals and delegations of procurement authority associated with investments in information technologies supporting agency application information systems.

504.1 Authorities.

(a) Chief Financial Officers Act (CFO Act).

(b) Clinger-Cohen Act of 1996, Public Law 104-106.

(c) Federal Acquisition Streamlining Act (FASA).

(d) Management of Federal Information Resources, Office of Management and Budget (OMB) Circular A-130.

(e) Acquisition of IRM Resources, USDA Departmental Regulation (DR) 3130-001, September 1995.

(f) Delegation of Procurement Authority for Information Technology, USDA Departmental Regulation (DR) 5039-7, September 1998.

(g) OMB Capital Planning Guide, June 1997.

(h) Planning, Budgeting, and Acquisition of Capital Assets, OMB Circular A-11, Part 3, July 2000.

(i) The Information Technology Architecture, OMB Publication M-97-16, June 1997.

(j) USDA Information Systems Technology Architecture Implementation and Management Plan, February 1997.

(k) USDA Guide to Information Technology Capital Planning and Investment Control, updated annually.

(l) Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-Making, US General Accounting Office, February 1997.

(m) Capital Planning and IT Investment Guide, US General Service Administration, February 2000.

504.2 Policy.

(a) NRCS will manage its investments in information technology for major application information systems (AIS) in accordance with Federal and departmental capital planning and investment control policies and procedures.

(b) NRCS will obtain system specific delegations of technical approval authority from the Department for major AISs used in conducting all of the agency's business.

(c) NRCS will manage acquisitions within the scope of each agency's AIS through the issuance of TA control numbers to ensure compliance with departmental, USDA Service Center, and NRCS technical architectures and capital investment plans.

(d) Technical Approval Authority.

(1) Organizational Units that wish to acquire NRCS IT resources must submit a Technical Approval (TA) request to the NRCS Technical Approval Manager located at the Information Technology Center, Fort Collins, Colorado.

(2) The preferred method for TA submission is on a AD-700 (standard requisition form) unless the Technical Approval Manager provides other instructions.

(3) While most TA requests are routine, requesting organizational units should be prepared to provided additional justification for unique or special purpose IT resources.

(4) TA is required for all hardware, software, and telecommunication components (hardware and software), including all upgrades (hardware and software) and maintenance expenditures. TA is Not Required for routine supplies; paper, printer/plotter cartridges, storage media (diskettes & tapes), miscellaneous cables and connectors; however, organizational units should maintain a record of funds expended for these items.

(5) Organizational units may request a TA report of their expenditures at any time by contacting the National TA Manager.

(e) Delegated Procurement Authority (DPA).

Acquisitions of all NRCS IT resources must be performed within the authorities granted or warranted to an individual. However, a specific delegation of procurement authority is required for all acquisitions exceeding $100,000 regardless of the warrant level of the individual. The $100,000 threshold is for acquisition price, not system life cycle costs. Delegation of procurement authority will not be issued prior to the issuance of a TA control number. The requester must initiate a specific request by following procedures in SCSR 5039-6.

504.3 Definitions.

(a) Application Information System. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures as part of one or more business processes. It includes hardware, software, personnel, telecommunications services, support services, and intra-governmental services.

(b) Delegated Procurement Authority (DPA). Authority to purchase IT resources. In this context, a delegation issued by the Director, Management Services Division, for those acquisitions defined in Part 504.2(e) above. This delegation has been granted from the Department to the Agency for issuance.

(c) Information Technology Architecture. A coherent collection of Federal and industry technical standards for hardware, software, telecommunications, security, and data that facilitates shared, distributed, integrated, and open systems.

(d) Information Technology (IT) Resources. Includes all IT equipment, IT services, IT software, IT support services, and IT related supplies.

(e) Technical Approval Authority. A delegation issued by the Department's Chief Information Officer (CIO), which authorizes an agency to acquire and/or use IT resources for commercial as well as in-house development and operation of an information system. Technical approval authority focuses on ensuring that IT acquisitions for AISs are technically sound and in conformance with specific information technology architecture that promotes interoperability, data sharing, and open communications. The issuance of TA is for a specific system life cycle. TA authority does not provide for funding of acquisitions.

(f) Technical Approval (TA) Control Number. A number issued to a requesting organizational unit upon receipt of an IT acquisition request. Technical approval control numbers are issued after verification that the requested IT resource complies with the scope and technical architecture for a specified application information system.

504.4 Responsibilities.

(a) The NRCS Chief Information Officer will:

(1) Obtain delegations of technical approval authority from the Department for application information systems covering all agency business areas.

(2) Report to the Department summaries of IT resource acquisitions by application information system and performance of that system against specific criteria.

(b) The Information Technology Center Director and National Technical Approval Manager will:

(1) Evaluate IT resource acquisition requests associated with agency application information systems for conformance to the technical architecture standard.

(2) Issue a TA control number for requests that meet the standards or justify why the request does not and provide alternatives to consider.

(3) Track IT resource acquisitions or expenditures for all agency application information systems and provide a report to the NRCS Chief Information Officer.

(4) Evaluate IT resources to ensure compatibility with USDA and/or NRCS approved technical architecture.

(5) Identify NRCS IT resource needs, which have the potential for consolidation and national buys, due to standardization and/or compatibility requirements, and recommend such action.

(c) The Information Technology Acquisition Team Leader will:

(1) Develop and maintain sources of available IT resources.

(2) Perform consolidated acquisitions and national purchases when:

(i) IT resources to be acquired are identified as favorable and conducive to a consolidated acquisition, and

(ii) The potential for volume purchases is in the best interest of the Government.

(3) Put new contracts in place for IT resources or arrange for NRCS to have access to other agencies' IT resource contracts.

(4) Review DPA requests and provide recommendations to the Management Services Division Director.

PART 505 - WAIVING INFORMATION TECHNOLOGY POLICY

505.0 Purpose.

505.1 Authorities.

505.2 Policy.

505.3 Definitions.

505.4 Responsibilities.

PART 505 - WAIVING INFORMATION TECHNOLOGY POLICY

505.0 Purpose.

To provide policy and responsibilities for documenting, submitting, and acknowledging requests for waivers to IT policy. Part 505 cancels National Instruction No. 270-305, dated May 1989.

505.1 Authorities.

(a) Management of Federal Information Resources, Office of Management and Budget (OMB) Circular A-130.

(b) Acquisition of IRM Resources, USDA Departmental Regulation (DR) 3130-001, September 1995.

(c) Delegation of Procurement Authority for Information Technology, USDA Departmental Regulation (DR) 5039-7, September 1998.

505.2 Policy.

(a) The NRCS Chief Information Officer (CIO) has the authority to approve waivers from NRCS information technology policy.

(b) The NRCS CIO will not grant waivers that are in violation of Federal and USDA governing policy and regulations.

(c) The requester must meet all other policy requirements that have not been specifically waived.

505.3 Definitions.

Waiver.

(a) A one-time approval granted for deviation from any NRCS IT policy.

(b) A request for additional and reasonable time granted to meet established policy.

505.4 Responsibilities.

(a) State Conservationists, Regional Conservationists, and Deputy Chiefs may request a waiver to NRCS IT policies by submitting a waiver request to the NRCS CIO in the following format:

(1) Purpose. State the reason for the waiver and why it is critical to the needs of the requesting organization. Include the circumstances of any previous waiver requests submitted from this organizational unit.

(2) Background. Provide the conditions leading up to this request and provide a thorough explanation of how policy is inhibiting the mission, goals, and objectives of the agency.

(3) Alternatives. Describe alternative approaches examined in resolving the matter. Include alternatives that would not resolve the matter.

(4) Proposed solution. State the recommended alternative that requires a waiver and reflect on how the solution will impact policy.

(5) Contact. State the name, title, location, and telephone number of the person to contact.

(6) Signatures. Sign the waiver request. The head of an organizational unit at the State level or above must sign the waiver request.

(b) The NRCS CIO will review requests on a case-by-case basis. Depending on the nature and complexity of the request, the CIO may request a review by IT and other non-IT technical staff.

PART 506 - GEOGRAPHIC INFORMATION SYSTEMS (GIS)

506.0 Purpose.

506.1 Authorities.

506.2 Policy.

506.3 Definitions.

506.4 Responsibilities.

PART 506 - GEOGRAPHIC INFORMATION SYSTEMS (GIS)

506.0 Purpose.

(a) To state policy, authorities, and responsibilities within the information resources management infrastructure for the implementation and use of GIS technology.

(b) To supplement related policy such as GM Section 170, Part 400 to address the cross-disciplinary requirements of a successful implementation of GIS technology.

506.1 Authorities.

(a) Management of Federal Information Resources, Office of Management and Budget (OMB) Circular A-130.

(b) Coordination of Surveying, Mapping, and Related Spatial Data Activities, OMB Circular A-16 (revised October 1990).

(c) Coordinating Geographical Data Acquisition and Access: The National Spatial Data Infrastructure, Executive Order 12906 (April 11, 1994).

(d) Computer Security Act of 1987, Public Law 100-235.

(e) Government Paperwork Elimination Act (GPEA), Public Law 105-277, October 1998.

(f) Federal Acquisition Reform Act (FARA).

(g) Clinger-Cohen Act of 1996, Public Law 104-106.

(h) General Manual Section 170, Part 400 entitled Cartography, Remote Sensing, Global Positioning and Geospatial Data Draft update 7/2000.

(i) Federal Geographic Data Committee (FGDC), Geospatial Data References.

(j) United States Department of Agriculture (USDA) Service Center Geographic Information System (GIS) Strategy, August 18, 1998.

(k) Standard for Geospatial Dataset File Naming, Service Center Database Team, March 2000.

(l) Service Center Modernization Plan of the USDA County Based Agencies, November 1999.

(m) Customer Service Toolkit Deployment Plan, May 2000.

(n) The National GPS Plan, IGEB, 1999.

(o) NRCS General Manual Title 140, Strategic Planning and Policy Analysis.

506.2 Policy.

(a) NRCS will use GIS technology to support conservation objectives and meet agency needs.

(b) NRCS offices shall effectively use procedures, standards, processes, equipment, software capabilities, and developments necessary for the utilization of GIS technology.

(c) NRCS will manage geospatial data, develop, maintain, and implement GIS software applications, according to the guidelines in Sections 505, 506, and 508 of the Rehabilitation Act of 1973 and subsequent amendments.

(d) Operational responsibility for GIS will reside with Regional and State Conservationists, and applicable directors at Centers, Institutes, and NHQ.

(e) NRCS will manage and integrate GIS in an interdisciplinary environment to achieve the most effective use of the technology.

(f) NRCS will coordinate GIS technology in cooperation with USDA agencies, other Federal agencies, and non-government partners to efficiently implement the technology to fulfill program requirements and conservation objectives.

506.3 Definitions.

(a) Cartography. The art and science of the organization and communication of geographically related information, such as soils data and maps. The term refers to their construction from data acquisition to presentation and use.

(b) Geographic Information Systems (GIS). Geographic information systems are a computer-based technology designed to input, manage, manipulate, analyze, and display geospatial data. In referencing the field of GIS, four key components must be satisfied to successfully implement the technology: software, hardware, people, and data.

(c) Remote Sensing. Remote Sensing is the science and art of obtaining information about an object, area, or phenomenon through the analysis of data acquired by a device that is not in contact with the object, area, or phenomenon under investigation. Examples of typical remote sensing products used by NRCS include aerial and satellite imagery and digital orthoimagery.

(d) Global Positioning Systems. The Global Positioning System (GPS) is a constellation of satellites providing users around the world with precise position, navigation, and time information 24 hours a day.

(e) Geospatial data. Geospatial data is information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the Earth. This information may be derived from a variety of sources including remote sensing, mapping, and GPS technologies.

506.4 Responsibilities.

(a) The Chief Information Officer (CIO) will:

(1) Provide national leadership for policy formulation relating to hardware and software requirements for GIS implementation within NRCS. Policy formulation is developed in cooperation with agency business experts and other USDA field-based agencies and partners.

(2) Assist in the coordination of GIS policy development among NRCS Federal and non-Federal partners.

(3) Provide policy and program leadership to the Information Technology Center (ITC) for geospatial related activities. Policy and priorities are developed collaboratively with business area experts, State, Regional, and national staff to ensure NRCS program requirements are met.

(4) Facilitate the collaborative management of geospatial hardware and software maintenance at all levels of the agency.

(5) Provide national leadership for the continued development of a telecommunications infrastructure throughout the agency which supports the use, application, and dissemination of geospatial data.

(6) Serves as NRCS Point of Contact (POC) for GIS Open Consortium.

(7) Facilitate collaborative partnerships with other Federal agencies and non-Federal partners to share telecommunication capabilities.

(b) The Director, Resource Inventory Division (RID) will:

(1) Develop policy, procedures, standards, and guidance for natural resource data collection (including the National Resource Inventory and other special inventories) and geospatial data collection, integration, utilization, and coordination. Provide coordination with others to ensure the efficient collection and integration of natural resources data across the agencies.

(2) Work closely with the Soil Survey Division regarding guidance for the National Cartography and Geospatial Center and for the National Aerial Photography and National Digital Orthophotography programs for those functions that support natural resource data collection activities.

(3) Work across Deputy Chief and division lines and with Regional and State conservationists, Institutes, and national centers to ensure that technical and program coordination takes place within the agency regarding the division's areas of responsibility.

(4) Plan, coordinate, and formulate budget requests and allocation of funds for assigned program activities and prepare analyses and justification statements for budget requests.

(5) Be responsible for the acquisition, management, and maintenance of the National Resource Inventory, hydrologic units, and related geospatial and attribute databases.

(6) Provide leadership and technical support for interagency coordination of geospatial natural resource data base development and data collection standards.

(7) Provide leadership and representation in natural resource data collection and geospatial sciences including cartography, remote sensing, and global positioning systems.

(8) Provide leadership for identifying and transmitting research needs within the division's areas of responsibility to research agencies and ensuring the dissemination and use of research findings.

(9) Provide technical leadership and direction for employee development and training in natural resource inventories and geospatial data bases and applications.

(10) Provide leadership and guidance for natural resource inventories based on strategic plan.

(11) Provide agency program and technical leadership to the Federal Geographic Data Committee (FGDC), National Aerial Photography Program (NAPP), National Digital Orthophoto Program (NDOP), Interagency Global Positioning System Executive Board (IGEB), USDA Remote Sensing Committee, National U.S. Atlas Steering Committee, Open GIS Consortium, and Advisory Council on Water Information (ACWI).

(c) The Information Technology Center (ITC) Director will:

(1) Develop, test, deploy, and support geospatial applications in cooperation and consultation with agency business experts and the CIO.

(2) Provide technical assistance to users for custom application software.

(3) Provide input/guidance for agency-wide software and hardware procurements related to geospatial technologies.

(4) Investigate, assess, and recommend new technology for GIS applications.

(d) The National Cartography & Geospatial Center (NCG) Director will:

(1) Provide cartography, remote sensing, GPS, and geospatial products, services, training, and data specific technical assistance.

(2) Provide quality assurance for cartography, remote sensing, GPS, and GIS products and geospatial data services in conformance with NRCS, Federal, and industry standards.

(3) Work closely with the Information Technology Center in the design, development, deployment, and application of technology relating to cartography, remote sensing, GPS, and geospatial data to support program requirements.

(4) Serve as the NRCS Geospatial Data Clearinghouse to archive and distribute agency geospatial data to support agency program needs, software application deployment, such as the Customer Service Toolkit and the National Spatial Data Infrastructure. See General Manual Section 170 for additional responsibilities.

(e) Regional Conservationists will:

(1) Maintain GIS expertise and ensure that the use of GIS technology is effective in Regional and National strategic planning and analysis.

(2) Ensure GIS activities comply with all Federal, USDA, and NRCS policies in regional strategic planning and analysis.

(f) State Conservationists will:

(1) Lead cartography, remote sensing, GPS, and GIS activities in the State.

(2) Designate principal State staff member(s) to serve as the State coordinator for cartography, remote sensing, GPS, geodata, and GIS activities.

(3) Maintain staff technical expertise in cartography, remote sensing, GPS, and geospatial technologies to support agency programs.

(4) Provide training in cartography, remote sensing, GPS, and GIS for appropriate staff.

(5) Provide software, hardware, staffing, and data support to field offices for the successful application of the Customer Service Toolkit in those locations where States chose to implement.

(6) Complete the development of key programmatic geospatial data layers to assist in State, Regional and national program management. Examples of such layers include Environmental Quality Improvement Program (EQIP), Wetlands Reserve Program (WRP), Resources Conservation and Development (RC&D), and Farmland Protection Program (FPP) boundaries.

(7) Ensure that GIS activities within the State comply with all Federal, USDA, and NRCS policies.

(8) Use an interdisciplinary environment to manage GIS technology and projects to achieve the most effective use of this technology.

(g) State GIS Specialists will:

(1) Provide cartography, remote sensing, and geospatial data products, services, and technical leadership in support of State NRCS programs and activities.

(2) Ensure that the appropriate security procedures are in effect to protect NRCS geospatial data. See General Manual Section 170 for greater detail.

PART 507 - DATA MANAGEMENT

507.0 Purpose.

507.1 Authorities.

507.2 Policy.

507.3 Definitions.

507.4 Assignment of Data Stewardship.

507.5 Responsibilities.

PART 507 - DATA MANAGEMENT

507.0 Purpose.

(a) To describe data management policy supporting the Natural Resources Conservation Service (NRCS) mission objectives and assign responsibility for the management, implementation, and the operation of the data management functions.

(b) Part 507 pertains to all national electronic data (attribute and spatial) that are operational, under development, and planned. It pertains to all data created, collected, processed, disseminated, or stored by the agency both directly and indirectly (e.g., through partnerships or contracts). It also applies to data obtained from outside sources to the extent that: 1) the data is made available to applicable users, and 2) that data stewardship responsibilities are exercised where NRCS can change or influence the content of this data. Refer to Section 120-Part 508 of the General Manual for policy on procedures governing non-electronic data.

(c) This policy and associated data management procedures, standards, and guidelines issued pursuant to this policy apply to all data utilized within National and/or Local databases developed, populated, or reengineered by any organizational unit of NRCS. Local databases fall under the responsibility of local managers, who have sole responsibility to provide the tools and environment for adequately managing and protecting local data stores critical to their mission. This policy also applies to contractors, consultants, partners, and universities providing the development and maintenance services to NRCS.

507.1 Authorities.

(a) Computer Security Act of 1987, Public Law 100-235.

(b) Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure, Executive Order 12906, April 11, 1994.

(c) Content Standard for Digital Geospatial Metadata, Federal Geographic Data Committee (FGDC), June 1998.

(d) Government Paperwork Elimination Act (GPEA), Public Law 105-277,

October 1998.

(e) Coordination of Surveying, Mapping and Related Spatial Data Activities, Office of Management and Budget (OMB) Circular A-16 (revised October 1990).

(f) Management of Federal Information Resources, OMB Circular A-130.

(g) Departmental Data Administration Program, USDA Departmental Regulation (DR) 3400-4, August 1994.

(h) Spatial Data Transfer Standard, FIPS 173-1.

(i) Standards and Guides published by the Interagency Service Center Data Team.

(j) NRCS Information Resources Management Strategic Long-Range Plan, USDA Natural Resources Conservation Service (annual USDA document).

(k) USDA Information Systems Technology Architecture, February 1997.

507.2 Policy.

(a) NRCS data are an important asset that has considerable value and must be managed with the attention that is accorded other agency assets. It is the policy of NRCS to implement data management in ways that enhance mission performance through the effective acquisition, integration, dissemination, and use of all data and metadata.

(b) Data and Metadata Quality.

NRCS will manage data and metadata to improve, maximize, and protect their quality. In the following list, "NRCS" refers to the appropriate management official. See Section 507.6 for managerial responsibilities.

(1) NRCS will ensure that policies, standards, and procedures regarding data quality are developed and procedures are implemented for each National Database.

(2) NRCS will establish authority and management responsibility for National Databases by assigning an Executive Data Sponsor and a Data Steward for each database. NRCS will ensure that these responsibilities are identified in performance plans and business plans.

(3) NRCS will establish authority and management responsibility for Local Databases.

(4) NRCS will provide training on data management roles and responsibilities with the goal of implementing effective data management.

(5) NRCS will ensure that databases are managed efficiently and effectively.

(6) NRCS will ensure that databases have effective security plans and operational procedures.

(c) Data Sharing.

All databases will be organized, integrated, and managed to promote the maximum utilization and sharing of data and information resources.

(1) NRCS will form partnerships and cooperative agreements with other USDA, Federal, and public organizations with which NRCS shares data.

(2) NRCS will use applicable Federal, USDA, and agency standards in defining and documenting databases and data elements.

(3) NRCS will utilize and maintain a metadata repository containing the official definition of the agency's National Databases, standard data elements, data models, and other metadata.

(d) Information Access.

NRCS will streamline information access by documenting and making information accessible as effortless and economical as possible. NRCS will make available through online access or standard computer media National Databases that contain data authorized for public release.

507.3 Definitions.

(a) Business Area.

An authorized program function or mission within an agency for which managerial responsibility has been delegated to an individual.

(b) Business Rule.

A statement that defines or constrains some aspect of the business as it is implemented in the data model (e.g. "an agency office can exist in only one location at a time"). Data-related business rules are statements, phrased in absolute terms, about data (e.g. "a telephone number must have 10 digits"), and about relationships between data (e.g. "if a phone number is entered, the phone type must also be entered".)

(c) Change Control.

Change control is an active management process that stabilizes the software development environment and protects systems/users who are dependent on particular data from being adversely impacted by changes to the definition, type, availability, or content of electronic data. The basic prerequisites for providing change control are:

(1) The establishment of management control over the definition of the data.

(2) A means to notify users that a change is being proposed

(3) A means to gather responses from dependent users and to assess the potential business impacts of the change. Note that the users may be programmers on the

project who are dependent on the format, availability, metadata, and stability of the data stores to complete their tasks.

(d) Common Data.

Data jointly owned, used, and managed by Service Center partners. All partner agencies can write to and update the dataset.

(e) Data.

A discrete fact or value. Data is the raw material which, through its use and interpretation, can provide valuable information. Data is the content of databases or data files.

(f) Data Administration.

Data administration encompasses the day-to-day technical functions that support ongoing business operations. Each application must implement a data administration process to support system development and ongoing system operation. It includes the collecting, defining, certifying, organizing, protecting, and delivery of both data and metadata (data about data).

(g) Data Administrator.

The person who defines, organizes, manages, controls, protects and standardizes data models, data elements, and metadata. Data administrators are a group of people appointed within the information technology area who jointly plan and administer the format, distribution, and storage of data. In this capacity, the Data Administrator translates the requirements of the Data Steward into a technical specification that can be programmed into an application system.

(h) Data Architecture.

An orderly arrangement of data resources to achieve:

```
(1)  A common understanding of available data resources.
(2)  A planned approach to data acquisition, storage, and retrieval to achieve a
high degree of responsiveness to user demands.
(3)  A high degree of data sharing and data mobility to reduce program delivery
costs.
```

(i) Data Dictionary.

A database about data and database structures. A catalog of all data elements containing their names, structures, and information about their usage. Normally, data dictionaries are

designed to store a limited set of available metadata, concentrating on the information relating to the data elements in the databases, files and programs of implemented systems.

(j) Data Management.

Data Management is the managerial function of taking responsibility for data and the processes that support it. It focuses the strategic planning and data methodologies for meeting program delivery goals. In particular, Data Management aims at managing data as an asset, particularly as a corporate asset. Data managers typically look across applications and business areas to manage the whole architecture of data resources for the enterprise.

(k) Data Mart.

A type of data warehouse that contains smaller subsets of data and focuses on a particular business discipline or organizational component.

(l) Data Model.

A pictorial view of data, groupings of data, and relationships between data groupings. A "logical" data model is a view that does not depend on the characteristics of the computerized system or of the physical storage. A "physical" data model typically refines the logical model by adding the constraints incumbent to the database system or physical storage method, and tuning the data model for access efficiency. A "business" data model typically identifies the main categories of data used and created by the application, integration points with other systems, data sources external to the enterprise, and known data structures that will be shared. A "conceptual" model is a further refinement of the "business" model, with greater detail, but not detailed specifics on data elements, tables, and other data stores.

(m) Data Repository.

A database of information describing the characteristics (metadata) of data. Typically, the repository also stores a broad range of descriptive information, including business rules, data models, and process models that help to elaborate on the usage of data in various systems. Repositories can also store metadata for the purpose of identifying and retrieving sets of actual data. Metadata that describes a map is an example.

(n) Data Steward.

A business area expert who is assigned responsibility for the data content of the database. The data steward establishes business rules, defines data elements, identifies valid data values, establishes certification standards, and ensures the completeness and availability of the data.

(o) Data User.

This category consists of all persons who use the data assets, including service center staff, service center customers, partner organizations, State and local governments, outside users of agency information, members of the agency business areas, and IT management and staff.

(p) Data Validation.

Applying a set of rules, comparisons, or decisions to a data element to determine if it falls within the pre-established boundaries of values for that element.

(q) Data Warehouse.

An informational database, or collection of databases, used to store shareable data. The warehouse is usually created through data extracts from operational databases. The warehouse adheres to a single enterprise data model to ensure consistency of decision-support data across the enterprise. The warehouse typically allows users to tap into an organization's vast store of operational data to track and respond to business trends, and to facilitate forecasting and planning efforts.

(r) Database.

A collection of related data organized to serve one or more applications. In the broader sense, it describes any organized collection of data regardless of the physical storage method.

(s) Database Administration.

The function of designing, implementing, securing, operating, and maintaining a collection of data in a database management system (DBMS). This includes the implementation of rules by which data is accessed and stored, performance monitoring, data backup and restoration, and the management of the DBMS software and its environment.

(t) Database Administrator.

The person who creates, manages, controls, and protects a database.

(u) Domain.

A list of all possible valid values for a data element. The domain can alternatively be expressed as a range of numeric or alphabetic values, or as a reference to an identified standard, such as a FIPS table.

(v) Enterprise Data Model.

An overall pictorial view of the participating agency's many applications and data assets. The intent is to manage the overall data assets to achieve optimal integration, sharing, access, and utilization of technology resources and infrastructure.

(w) Executive Sponsor.

A business-area manager who is accountable for the collection, management, and use of data assets. The Executive Sponsor is the person who determines that data, and the software to collect and manage the data, are necessary to fulfill the business-area mission.

(x) Geospatial Data.

Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth. This information may be derived from sources such as remote sensing, mapping, and surveying technologies. It includes both attribute (text) as well as spatial (map) data.

(y) Information.

A commodity derived from data through analysis or by the orderly presentation of data for human interpretation.

(z) Metadata.

Data about data. Metadata describes how, when, and by whom a particular set of data was collected, and how the data is formatted. Metadata includes attributes such as data name, length, domain of valid values, and definition. Metadata can also identify and describe a set of data or a complex data type such as a map, photograph, spatial data set, etc.

(aa) National Business-Area Data Steward.

The National Business-Area Data Steward has the ultimate responsibility for the definition of a data element, the business rules for creating the data, and the proper distribution and usage of the data. The Data Steward must therefore take an active role in the system creation and ongoing management. When the information system is operational, the Steward must actively monitor the creation and validation of the data.

The Business-Area Data Steward is also responsible for the content of a database or dataset. The Data Steward establishes definitions and domains for data elements; sets the procedures for collecting and certifying data and metadata; and manages the overall storage, maintenance, and distribution of the data and metadata. This person often acts as a

conduit between the end-user community and the IT community. The Data Steward may have frequent contacts with data administrators, application development teams, and database administrators supporting the business area.

(bb) National Database.

A permanent database that (1) has international, national, USDA, or agency-wide application, (2) is included in a standard software suite, (3) contains data that is used/shared directly in making national program decisions, or (4) is used/shared in multiple offices, States, or other internal/external organizations.

(cc) Shared Data.

Data owned and managed by a specific service center partner and shared by other partners. Usually, only the owning agency writes to the dataset, while other agencies can read the data.

(dd) Standard Data Element.

An element or structure that has a definition acknowledged by all partner agencies.

(ee) Unique Data.

Data owned and managed by a specific service center partner and not shared. The data is usually mission-specific, and is written and read only by the mission area of the particular agency.

507.4 Assignment of Data Stewardship.

(a) National Business-Area Data Stewardship.

(1) Data Stewardship occurs wherever data is stored. Each application will have a National Steward who reports directly to the project's Executive Sponsor. The National Steward is involved in the initial creation of the system, as well as the ongoing operation of the implemented system. If data is collected and stored at State and field locations, local data stewards will be appointed for those portions of the data.

(2) Individual NRCS offices may be supported by a multitude of national and local Data Stewards, each of whom is responsible for a piece of the total business going on within the office.

(b) Local Data Stewardship.

(1) A Local Data Steward will be assigned at each point in the organization where data is stored. The same person can be assigned for multiple storage points, or it can be different people. If data is widely distributed, stewardship must expand to cover it. Stewardship responsibility follows the data wherever it goes.

(2) Local Data Stewards are delegated specific responsibilities by the Business-Area Data Steward. These responsibilities may range from control and oversight of data collection and maintenance for an entire State to protecting a copy of a small subset of data used within a particular Service Center. Local Data Stewards should come from the business-area staffs at regional, State, area, or local offices. However, this responsibility may be delegated to someone outside the business-area, including an information technology person or a data user. At local levels, for example, this responsibility may be assigned to a service center employee who is not directly part of the business-area, but who uses data from multiple business areas in providing services to the public. All delegations of responsibility for data should be completed formally, either by letter or through position descriptions and performance elements.

(3) When copies or subsets of data are stored at State, Regional, or county offices, at universities, or with local governments, the Business-Area Data Steward and the Executive Sponsor need to establish Local Data Stewards to maintain these datasets. Data assets must always be within the span of control of the responsible business area, or their delegates, wherever this data is located. Copies of data may be released to outside parties, but only under conditions established by the business area to ensure the integrity of the data and the protection of privacy, data sensitivity, and security.

(4) Collaboration and communication must take place among data stewards at all levels of the organization to ensure that data assets of the enterprise are protected, maintained, and used as intended. This is particularly true when data moves between machines and offices.

507.5 Responsibilities.

(a) The Chief of the Natural Resources Conservation Service (NRCS) will:

(1) Provide resources to adequately administer the NRCS data management program.

(2) Provide the necessary resources to actively participate in the undertaking of Federal Geographic Data Committee (FGDC), including implementation of Executive Order 12906 and other Federal Regulations.

(3) Ensure that data management is an integral part of the overall mission planning.

(b) The Information Resources Management Review Board (IRB) will:

(1) Review and recommend data management policy for the agency.

(2) Recommend agency funding levels and establish priorities for development and the maintenance of national data collection programs and management of agency data assets.

(3) Foster and support standards and processes that enable interoperability of hardware, software, and data sharing.

(c) The NRCS Chief Information Officer (CIO) will:

(1) Ensure compliance with and development, coordination, and implementation of data management policies, procedures, rules, standards, and guidelines which involve planning, management, and control of NRCS data resources.

(2) Assess the agency data management program and include it in the business plan steps to improve effectiveness.

(3) Coordinate with the USDA, Federal data committees, partners, and NRCS program leadership on data management issues.

(4) Coordinate the development and management of metadata and provide an infrastructure for the orderly dissemination of data to the public.

(5) Manage the NRCS data security program.

(6) Provide for training in the effective management of data assets to managers at all levels of the organization.

(7) Provide data management guidance through the development and maintenance of topical standards, guides, and handbooks.

(d) The Director of the Information Technology Center (ITC) will:

(1) Provide technical leadership for implementing and managing the agency's technical and data architectures, and data management tools (hardware, software, physical data location, and movement of the data).

(2) Coordinate the design, integration, development, implementation, maintenance and support of application systems that manage data in National databases.

(3) Provide support for database design, development, and implementation.

(4) Coordinate information technology support service contracts.

(5) Maintain a central repository of metadata that describes the national data and national database assets.

(6) Investigate and recommend to the CIO and IRB appropriate data management technologies for the storage, management, conversion, integration, and dissemination of complex data types to support the agency mission.

(7) Support the implementation of intergovernmental and industry standards for the open interchange of spatial and attribute data.

(8) Support appropriate technology for the dissemination of data to agency customers and partners.

(e) The Director of the National Cartography and Geospatial Center (NCG) will:

(1) Manage the acquisition and dissemination of geospatial data and metadata.

(2) In conjunction with the Director, ITC, provide a clearinghouse for delivery of agency geospatial data and metadata, and information regarding availability of data to NRCS, other Federal, State, local agencies, other partners, and the general public.

(f) Executive Sponsors will:

(1) Determine that data is a necessary commodity for achieving the mission. The sponsor assumes overall responsibility for:

(i) Coordinating funding for data collection, storage, and maintenance, and for software application development, support, and maintenance;

(ii) Establishing standards and policies for the acquisition and certification of data;

(iii) Establishing the business definition of the data;

(iv) Ensuring protection of the physical data assets.

(2) Share responsibility between several business-area managers from different agencies or different parts of the same agency (in some cases).

(3) Appoint a Data Steward to handle the day-to-day coordination of data management responsibilities, and "contracts" for a project manager to oversee the development and maintenance of software applications.

(g) Regional Conservationists, State Conservationists, Center Directors, and NRCS Division Directors will:

(1) Act as the Executive Sponsor to manage local databases developed by their staffs to support activities within the region, individual State, center, or division.

(2) Support the administration and stewardship of national databases used by their organizational unit.

(h) The Data Steward(s) within a business area will:

(1) Manage and administer data needed to support the mission.

(2) Authorize individual customer access to data and set any limitations on that access (read/update/access to subsets/etc.).

(3) Determine which reports/data-extracts represent official agency information.

(4) Resolve disputes as to the meaning and valid use of data elements and values.

(5) Cooperate with fellow Data Stewards and the Data Team to develop, modify, approve, and enforce policies relating to the use and distribution of data resources.

(6) Formally delegate Data Steward's duties to others where appropriate so that individual responsibilities are clearly defined.

(7) Act as the designated authority for business-area decisions concerning data content and requirements for supporting software systems.

(8) Develop technical procedures for acquiring, collecting, archiving, and disseminating both data and metadata, including establishing cooperative agreements with outside sources of data.

(9) Develop and implement defensible quality assurance standards for data collection and management, and a quality control process to certify that standards have been met.

(10) For geospatial data, ensure that metadata is documented, approved, certified for release and made available through the clearinghouse network according to the current Federal Geographic Data Committee (FGDC) metadata standards.

(11) Coordinate with the ISSPM to identify security requirements for any information that may be excluded by the provisions of the Freedom of Information Act or must be protected under the Privacy Act.

(12) Identify training needs, develop training plans, develop training materials, and train users on use and management of the data.

(13) Certify that software applications meet subject matter and technical accuracy requirements.

(14) Coordinate with other USDA agencies and offices in setting development priorities and activities, and data accuracy and usage standards.

(15) Provide help desk support to governmental and outside users of data resources.

(i) Data Manager will:

(1) Provide a coordinating and oversight function over the data resources of multiple applications.

(2) At the request of the project manager, provide direct support to a specific project. This support could include requirements development, data modeling, planning, metadata development, and quality assurance.

(j) Data Administrator will typically:

(1) Create models of the system showing the processes and data stores it will contain.

(2) Create the logical organization of data elements and related metadata that forms the basis for physical file layouts and database schemas.

(3) Provide technical reviews and testing to ensure that the software correctly processes the data. With the Data Steward, establish the plan for migration of legacy data to the new system.

(4) Manage the technical aspects of the protection and delivery of production data.

(5) Maintain the model and technical documentation during the deployment and maintenance phases of the system.

(k) Database Administrator will:

(1) Act as the designated authority for decisions concerning the modeling, construction, and operation of a database

(2) Coordinate with system developers to establish the most effective database software, hardware configuration, and data storage distribution.

(3) Support the data steward in implementing customer access to data.

(4) Develop technical procedures and components for storing and accessing data and metadata.

(l) Data Collector will:

(1) Gather data to meet the business area mission.

(2) Collect and document metadata required to describe data being collected.

(3) Ensure the accuracy of data and metadata to the extent possible.

(4) Ensure accuracy in the initial entry of raw data into automated systems and databases.

(m) Data User will:

(1) Use data in the way it is intended to be used.

(2) Take responsibility for finding out the proper definition and usage of data.

(3) Provide information that allows data related to the user to be extracted and correlated.

(4) Take steps (security, login ID's, etc.) necessary to establish access to data stores.

PART 508 - SOFTWARE DEVELOPMENT

SUBPART A – GENERAL

PART 508 - SOFTWARE DEVELOPMENT

SUBPART A – GENERAL

508.0 Purpose.

To establish policies and procedures applicable to all software development in or for NRCS.

508.1 Authorities.

(a) Application Portability Profile (APP): The U.S. Government's Open Systems Environment Profile OSE/1, Version 2.0.

(b) Common Computing Environment (CCE) Information Technology Architecture (ITA).

(c) NRCS Data Rich and Information Poor, November 1995.

(d) NRCS Future Directions: An Overview-A Vision of Information Technology for Field Conservationists, August 1997.

(e) Standard Portable Operating System Interface for Computer Environments (POSIX), IEEE Std 1003.x, Institute of Electrical and Electronics Engineers (IEEE).

(f) Acquisition of IRM Resources, USDA Departmental Regulation (DR) 3130-001, September 1995.

(g) USDA Guide to Information Technology Capital Planning and Investment Control, March 2000.

(h) USDA Information Systems Technology Architecture, Version 1.0, February 1997.

508.2 Policy.

(a) The Information Resources Management Review Board (IRB) approves the development, acquisition, maintenance, and support of all NRCS national software.

(b) NRCS shall acquire cost effective, mainstream commercial-off-the-shelf (COTS) software when it meets the business needs of the agency.

(c) All NRCS software will conform to the USDA Information Systems Technology Architecture.

(d) All NRCS software for Service Center use shall be acquired or built to operate on the Common Computing Environment (CCE) information technology architecture.

(e) NRCS shall use an interdisciplinary approach to manage its software development projects to ensure that information technology policies are adhered to and that business area needs are met.

(f) All NRCS software development projects shall comply with applicable Federal, departmental, and agency information system and software development policies. In particular, all application software must conform to the NRCS technical approval requirements and procedures.

(g) NRCS shall coordinate the implementation of all agency national software that addresses overlapping business areas in Service Centers with the Farm Service Agency, Rural Development, and other conservation partners.

508.3 Definitions.

Application Software. Commercial or custom software that is or will be deployed and used to conduct agency business. Software applications automate business processes, including processes that manage data and databases. Packages typically include an installation script, executable code, and user documentation. Custom agency-owned packages include a data model, data schema, data base scripts of record, data dictionary, system requirements, design documentation, source code files, and other system life cycle components.

508.4 Responsibilities.

(a) The NRCS Chief Information Officer (CIO) will:

(1) Provide policy and direction for application software development and integration within NRCS, with USDA Service Center partners, and with conservation partners.

(2) Ensure compliance with applicable Federal, departmental, and agency information system and software development policies.

(3) Provide policy and program leadership to national software development effort.

(b) The Information Resources Management Review Board (IRB) will approve information systems and applications and prioritize resource allocation to develop and maintain these systems.

(c) The Information Technology Center (ITC) Director will:

(1) Develop, integrate, deploy, and support national software.

(2) Provide consultation and training assistance to regions and States in local software development efforts.

(3) Manage the technical approval process.

(d) Regional Conservationists will:

(1) Organize and provide support for agency application software within their region.

(2) Provide IT/IRM staff to support information technology functions within the region, including application software development to meet specific State and local automation needs.

(3) Coordinate application software development within their regions.

SUBPART B - MANAGEMENT OF PROJECTS

PART 508 - SOFTWARE DEVELOPMENT

SUBPART B - MANAGEMENT OF PROJECTS

508.10 Purpose.

To describe policy and responsibilities for life cycle software management.

508.11 References.

(a) Capability Maturity Model (CMM), Software Engineering Institute (SEI).

(b) Management Application Systems Life Cycle Management, USDA Departmental Manual (DM), 3200-1, March 1988.

(c) Departmental Long Range IRM Planning, USDA Departmental Regulation (DR) 3111-001, February 1989.

(d) Software Management, USDA Departmental Regulation (DR) 3220-003, March 1988.

508.12 Policy.

(a) Application Systems Life Cycle (ASLC) Management, as defined in DM 3200-1, must be applied to all application software and database development projects where the application is deployed and supported in two or more States.

(b) All NRCS national, State, and local application software will be developed in accordance with a national set of software development standards.

508.13 Definitions.

Application Systems Life Cycle (ASLC). A set of standards for initiating, designing, installing, and maintaining applications systems. It provides a common framework for managing the system development and maintenance process. ASLC improves communication among diverse interest groups, facilitates control of the process, and specifies the contents of deliverables. The ASLC alerts management when a development project is in jeopardy.

508.14 Responsibilities.

(a) The NRCS Chief Information Officer will provide policy and direction for the development, implementation, and support of the NRCS application systems life cycle.

(b) The Information Technology Center Director will:

(1) Apply ASLC management process requirements to application software development under the ITC control.

(2) Employ consistent and formal project management practices to estimate, schedule, monitor, and adjust system life cycle workload for application software under the ITC control.

(3) Provide ASLC guidance, assistance, and quality assurance to software development efforts external to the Information Technology Center. Efforts include projects within NRCS regions and States, and with conservation partners where the products produced integrate with agency information systems.

(c) Agency line officers will apply ASLC management process requirements to application software development under their control. Employ consistent and formal project management practices to estimate, schedule, monitor, and adjust system life cycle workload for application software under their control.

SUBPART C - INFORMATION SYSTEMS INVENTORY

508.20 Purpose.

508.21 Authorities.

508.22 Policy.

508.23 Definitions.

508.24 Responsibilities.

PART 508 - SOFTWARE DEVELOPMENT

SUBPART C - INFORMATION SYSTEMS INVENTORY

508.20 Purpose.

To describe policy and responsibilities for maintaining and updating the NRCS information systems inventory.

508.21 Authorities.

Management of Federal Information Resources, Office of Management and Budget (OMB) Circular A-130.

508.22 Policy.

(a) NRCS will maintain an inventory of the agency's major information systems, holdings, and information dissemination products.

(b) The contents of the inventory will be available to NRCS staff and NRCS partners, and others when appropriate.

508.23 Definitions.

Dissemination. The term "dissemination" means the government initiated distribution of information to the public.

508.24 Responsibilities.

(a) The NRCS Chief Information Officer will:

(1) Provide policy and direction for the development, implementation, and support of the NRCS IT systems inventory.

(2) Ensure that the NRCS IT systems inventory contains current information and that inventory information is readily available to users.

(b) The Information Technology Center Director will:

(1) Develop and maintain an NRCS IT systems inventory database.

(2) Maintain an inventory of ITC developed applications and NRCS applications to be deployed on the Service Center Common Computing Environment.

(3) Keep the inventory data current and develop reports as needed.

(c) Agency line officers will ensure that IT systems inventory data is current and accurate.

SUBPART D - OUTSIDE SERVICES

508.30 Purpose.

508.31 Authorities.

508.32 Policy.

508.33 Responsibilities.

PART 508 - SOFTWARE DEVELOPMENT

SUBPART D - OUTSIDE SERVICES

508.30 Purpose.

To establish policies and responsibilities applicable to the use of outside services in software development, both for contracts with commercial vendors and cooperative agreements with agencies external to NRCS, both Federal and non-Federal.

508.31 Authorities.

Federal Acquisition Regulations (FAR).

508.32 Policy.

(a) NRCS may use external resources to produce application software system life cycle deliverables and support NRCS IT systems. All external resources must be managed by Federal employees.

(b) Contract support services and cooperative agreements must be executed within Federal, departmental, and agency policy for procurement and other applicable management services. In particular, NRCS technical approval requirements and processes must be satisfied.

508.33 Responsibilities.

(a) The Information Resources Management Review Board (IRB) will assess requests and approve allocation of agency resources for support services contracts and cooperative agreements to deliver specified application software system life cycle products and support.

(b) The NRCS Chief Information Officer will:

(1) Provide policy and direction for the use of outside support services.

(2) Develop information technology strategies that may include the use of outside services to meet agency needs for application software.

(c) The Management Services Division Information Technology Acquisition Team (ITAT) will:

(1) Establish and manage contracts for outside services.

(2) Maintain a contract file for all deliverables specified in contracts.

(3) Provide the Contract Officer for all contracts.

(4) Work with requesting office to appoint a Contracting Officer Technical Representative (COTR).

(d) The Information Technology Center Director will:

(1) Provide the technical expertise and assistance to the ITAT for establishing and maintaining contracts for outside services.

(2) Provide assistance to the ITAT in developing the request for proposal (RFP) and/or Statement of Work (SOW) needed to acquire outside services.

(e) Agency line officers will establish and manage contracts for outside services within their area of jurisdiction.

PART 509 - NATIONAL SOFTWARE AND HARDWARE TESTING, CERTIFICATION AND DISTRIBUTION

SUBPART A - SOFTWARE TESTING

PART 509 – NATIONAL SOFTWARE AND HARDWARE TESTING, CERTIFICATION AND DISTRIBUTION

SUBPART A - SOFTWARE TESTING

509.0 Purpose.

This subpart provides policy for testing NRCS developed software including software developed in cooperation with other Federal, State, and local governments, universities, etc.

509.1 References.

(a) IEEE Standard for Software Test Documentation, IEEE Std 829-1998.

(b) IEEE Standard for Software Unit Testing, IEEE Std 1008-1987 (R1993).

(c) IEEE Standard for Software Verification and Validation, IEEE Std 1012-1996.

(d) Supplement to IEEE Standard for Software Verification and Validation: Content Map to; IEEE/EIA 12207.1-1997, IEEE Std 1012a-1998.

(e) IEEE Guide for Software Verification and Validation Plans, IEEE Std 1059-1993.

(f) Information Technology – Software Packages – Quality Requirements and Testing, IEEE Std 1465-1998.

(g) USDA Service Center Agencies Policies for Hardware Configuration, Application Submissions, and Change Control Policy, June 30, 2000.

509.2 Policy.

(a) All NRCS custom developed software for use by NRCS personnel shall be tested. References listed in Section 509.1 shall be used as needed.

(b) Various types of testing for an application system are defined in Section 509.3. NRCS shall use the various types of testing as required to ensure the highest probability of success in implementing an application system.

(c) NRCS custom software developed by a State, region, Center, Institute, NHQ, or other organizational unit for use within that particular organizational unit shall be tested by the State, region, Center, Institute, NHQ, or other organizational unit, respectively. If testing resources are unavailable at the organizational level, then the ITC Software Testing Laboratory (STL) shall test the software.

(d) All NRCS software, whether custom developed or commercial-off-the-shelf (COTS), to be installed on or executed from the service center common computing environment shall undergo interoperability testing and shall be certified by one of the following: ITC Software Testing Laboratory, Farm Service Agency (FSA) Kansas City Management Office (KCMO), or the Interoperability Lab (IOL) in Beltsville, Maryland.

509.3 Definitions.

(a) Acceptance testing. Testing conducted in an operational environment to determine whether a system satisfies its acceptance criteria and to enable the customer to determine whether to accept the system. This testing is client or user oriented (often referred to as "beta" or "field" testing).

(b) Component testing. Testing to verify the correct implementation of the design and compliance with program requirements of one software element (e.g., unit, module) or a collection of software elements.

(c) Integration testing. An orderly progression of testing of incremental pieces of the software program in which software elements, hardware elements, or both are combined and tested until the entire system has been integrated to show compliance with the program design, and with the capabilities and requirements of the system.

(d) System testing. The activities of testing an integrated hardware and software system to verify and validate whether the system meets its original objectives.

(e) Interoperability testing. The highest level of application testing performed on a completely assembled product to ensure the application can be installed/de-installed and can co-exist with other applications on an established configuration.

509.4 Responsibilities.

(a) The Project Managers will:

(1) Ensure that software has been adequately tested.

(2) Ensure that software to be installed on the Common Computing Environment (CCE) platform has been submitted and certified by one of the following: ITC Software Testing Laboratory, Farm Service Agency (FSA) Kansas City Management Office (KCMO), or the Interoperability Lab (IOL) in Beltsville, Maryland.

(b) The Director of the Information Technology Center will conduct an annual review of the effectiveness of the software testing procedures. The results of the annual review will be provided to the NRCS Chief Information Officer (CIO).

SUBPART B - SOFTWARE CERTIFICATION AND DISTRIBUTION

509.10 Purpose.

509.11 Authorities.

509.12 Policy.

509.13 Duplication and Distribution.

509.14 Responsibilities.

509.15 Requests for Software.

PART 509 - NATIONAL SOFTWARE AND HARDWARE TESTING, CERTIFICATION AND DISTRIBUTION

SUBPART B - SOFTWARE CERTIFICATION AND DISTRIBUTION

509.10 Purpose.

This subpart provides policy for the certification and distribution of software.

509.11 Authorities.

USDA Service Center Agencies Policies for Hardware Configuration, Application Submissions, and Change Control Policy, June 2000.

509.12 Policy.

(a) All NRCS custom developed software shall be certified for release by the executive sponsor or organizational unit responsible for the development of the product (i.e., State, regional, or national IRM official). The software release shall include documentation of all known problems and work-arounds associated with the software and its installation.

(b) All NRCS custom developed software for national use shall be formally released via a letter signed jointly by the Director of the ITC and the executive sponsor of the application.

(c) Support issues for national use software shall be coordinated with the National Help Desk before distribution of the software.

(d) All software distributed within a State shall be approved by the State IRM official.

509.13 Duplication and Distribution.

(a) All national software, including documentation materials, will be distributed by the NRCS organizational unit that originally developed the software.

(b) All national software to be installed on or executed from a service center common computing environment shall be distributed by the ITC in accordance with the Service Center common computing environment policies and procedures. CCE documentation is available at http://www.sci.usda.gov/cce/guides.html.

509.14 Responsibilities.

The software executive sponsor or other authorized person will:

(a) Coordinate with the State IRM official to certify and distribute software developed to be used within the confines of a State.

(b) Coordinate with the Director of the ITC to certify and distribute software developed to be used across State boundaries.

509.15 Requests for Software.

NRCS developed software is public domain. Requests for software from outside sources will be handled by the Freedom of Information Act Officer.

SUBPART C - HARDWARE TESTING AND INTEGRATION

509.20 Purpose.

509.21 References.

509.22 Policy.

509.23 Responsibilities.

PART 509 - NATIONAL SOFTWARE AND HARDWARE TESTING, CERTIFICATION AND DISTRIBUTION

SUBPART C - HARDWARE TESTING AND INTEGRATION

509.20 Purpose.

This subpart provides policy for testing, evaluating, and certifying computer hardware and telecommunications systems proposed for use within NRCS.

509.21 References.

Service Center Agencies Policies for Hardware Configuration and Application Submissions and Change Control Policy, June 2000.

509.22 Policy.

(a) All new hardware and telecommunications systems proposed for use by agency personnel shall be tested, evaluated, and certified that the systems meet agency requirements.

(b) Systems and applications software designed to run on agency approved platforms shall be tested and evaluated in conjunction with the service center common computing environment policies and practices.

(c) Systems shall be tested in accordance with NRCS standard testing and benchmarking procedures.

(d) Upon completion of formal testing and evaluation, systems will be certified for use by the agency.

509.23 Responsibilities.

The requesting office is responsible for ensuring that hardware and telecommunications systems are tested in accordance with 509.22.

PART 510 - CONFIGURATION MANAGEMENT

510.0 Purpose.

510.1 Authorities.

510.2 Policy.

510.3 Definitions.

PART 510 - CONFIGURATION MANAGEMENT

510.0 Purpose.

To establish policy for software and hardware configuration management.

510.1 Authorities.

(a) IEEE Standard for Software Configuration Management Plans, IEEE Standard 828-1998.

(b) IEEE Guide to Software Configuration Management, IEEE Standard 1042-1987 (Reaff 1993).

(c) IEEE Standard for Software Productivity Metrics, IEEE Standard 1045-1992.

(d) IEEE Standard for Software Reviews, IEEE Standard 1028-1997.

(e) ISO 10007 Guidelines for Configuration Management.

(f) SEI Capability Maturity Model.

(g) Service Center Agencies Policies for Hardware Configuration and Application Submissions and Change Control Policy, June 2000.

510.2 Policy.

(a) NRCS will implement configuration management on all major software development projects as part of the Application Systems Life Cycle (ASLC).

(b) NRCS will ensure only personnel responsible for configuration management will install system changes.

(c) NRCS will ensure that any changes in configuration managed items follow the procedures outlined in Configuration Managed Items Change Request Policy.

510.3 Definitions.

(a) Configuration Management (CM). Configuration management is a discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, control changes to those

characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.

(b) Quality Assurance (QA). Quality assurance is a planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. QA is also a set of activities designed to evaluate the process by which the products are developed.

(c) Version Control. Software that has both a time history as well as numerical sequencing such that whole applications can be repeated and reliably built and maintained.

(d) Version Description Document (VDD). Version description document is a document that accompanies and identifies a given version of a system or a component.

510.4 Responsibilities.

(a) The Information Technology Center Director will annually review the effectiveness of the configuration management process in cooperation with the Chief Information Officer.

(b) The Interoperability Laboratory Manager:

(1) Has responsibility for configuration management of all CCE hardware and software.

(2) Will ensure that all current USDA Service Center Agencies policies and procedures for configuration management are followed.

510.4 Responsibilities.

PART 511 - INFORMATION SYSTEM LIFE CYCLE OVERSIGHT AND EVALUATION

511.0 Purpose.

511.1 Authorities.

511.2 Policy.

511.3 Definitions.

511.4 Responsibilities.

PART 511 – INFORMATION SYSTEM LIFE CYCLE OVERSIGHT AND EVALUATION

511.0 Purpose.

To establish policy for information technology oversight and evaluation of NRCS information systems.

511.1 Authorities.

(a) Standard Dictionary of Measures to Produce Reliable Software, IEEE Standard 982.1-1988.

(b) IEEE Standard for the Use of Standard Dictionary of Measures to Produce Reliable Software, IEEE Standard 982.2-1988.

(c) IEEE Standard for Software Reviews, IEEE Standard 1028-1997.

(d) IEEE Standard for Project Management Plans, IEEE Standard 1058-1998.

(e) IEEE Guide to the Project Management Body of Knowledge, IEEE Standard 1490.

(f) Management Application Systems Life Cycle Management, USDA Departmental Manual (DM) 3200-1, March 1988.

(g) IRM Review Program, USDA Departmental Regulation (DR) 3150-002, January 1989.

511.2 Policy.

(a) Periodic audits of NRCS information systems shall be conducted to assess compliance with IEEE and other appropriate information technology standards referenced in 511.1 above and in Part 508.

(b) Each primary NRCS information system shall be audited at least once within each five (5) year period of its life cycle.

511.3 Definitions.

Information System Life Cycle Management. The process of administering an information system over its entire life cycle. An information system contains the components developed and maintained during its lifecycle, including hardware and software configurations,

application architecture, technical architecture, custom software components, application built packages, databases, project plans, test plans, implementation and migration plans, system documentation, and user documentation. The life cycle is the time span between establishing the need for the system and the end of its operational use. The life cycle is divided into discrete or separate phases with formal milestones used as points of management control.

511.4 Responsibilities.

NRCS Chief Information Officer will:

(a) Determine the need for, schedule, and select teams to perform audits of NRCS information systems.

(b) Ensure that follow-up agreed-to actions from audits are implemented in all NRCS primary information systems.

PART 512 - TELECOMMUNICATIONS MANAGEMENT

SUBPART A – GENERAL

PART 512 – TELECOMMUNICATIONS MANAGEMENT

SUBPART A - GENERAL

512.0 Purpose.

To outline general roles and responsibilities for the acquisition, management, and integration of telecommunications services, equipment, and facilities.

512.1 Authorities.

Telecommunications and Internet Services and Use, USDA Departmental Regulation (DR) 3300-001, March 1999.

512.2 Definitions.

(a) Telecommunications. Any transmission, emission, or reception of signs, signals, writing, images, and sounds of information of any nature by wire, radio, visual, or other electromagnetic systems.

(b) FTS2001. Non-mandatory Federal telecommunications contract awarded by GSA to replace the FTS2000 contract. The FT2001 contracts were awarded with a minimum revenue guarantee (MRG) to each vendor.

512.3 Responsibilities.

(a) The Information Technology Division Director will work with the NRCS Telecommunications Mission Area Control Officer (TMACO) to develop and distribute telecommunications policy.

(b) The Information Technology Center (ITC) Director will manage and coordinate the acquisition, use, and disposal of telecommunications services and equipment.

(c) The NRCS Telecommunications Mission Area Control Officer (TMACO), ITC will:

(1) In consultation with the Information Technology Division and the Information Technology Center, establish policies and procedures for the management and cost control of telecommunication systems.

(2) Provide advice and assistance to offices regarding telecommunications services and facilities in support of program requirements.

(3) Evaluate and approve or disapprove all requests received for telecommunications services and equipment.

(4) Coordinate telecommunications planning with the NRCS IRM Strategic Long-Range Plan and prepare an "IRM objective" for telecommunications as part of the plan.

(5) Serve as the single point-of-contact for all matters relating to telecommunications.

(6) Maintain familiarity with Emergency Program Telecommunications requirements.

(7) Ensure that the development of telecommunications facilities and services are in accordance with departmental policies.

(8) Serve as the NRCS FTS2001 Coordinator.

(d) Division Directors, Regional Conservationists, State Conservationists, and other heads of NRCS offices will:

(1) Ensure compliance with all requirements specified in this Part as well as other governing regulations.

(2) Appoint IRM coordinators at regional and State offices to serve as the primary points-of-contact for all matters relating to telecommunications.

SUBPART B - FTS2001

512.10 Purpose.

512.11 Authorities.

512.12 Policy.

512.13 Definitions.

512.14 Responsibilities.

PART 512 - TELECOMMUNICATIONS MANAGEMENT

SUBPART B - FTS2001

512.10 Purpose.

To establish policy for FTS2001.

512.11 Authorities.

(a) FTS2001 Reference Guide.

(b) General Services Administration (GSA) FTS2001 Agency Reference Guide.

512.12 Policy.

(a) FTS2001 shall be used to satisfy core long distance service (Inter-LATA) requirements. In DR3300-1, core services are defined as mandatory services until Vendor MRG is met.

(b) Where FTS2001 meets long distance telecommunications requirements, technical approval (TA) is not necessary. However, the TMACO must approve all requests.

(c) All requests for waivers from the FTS2001 contract must be submitted to the TMACO.

512.13 Definitions.

FTS2001 Core Services. The FTS2001 Core services are:

(a) Switched Voice Service.

(b) Circuit Switched Data service (Packet Switched Service, Frame Relay, Asynchronous Transfer Mode, and Internet Protocol Service).

(c) Toll Free Service.

(d) Compressed Video Service.

(e) Dedicated Transmission Service.

512.14 Responsibilities.

(a) The Telecommunications Mission Area Control Officer (TMACO) will:

(1) Serve as the sole signature authority to approve the ordering of dedicated network access services and equipment.

(2) Facilitate the engineering of dedicated network access arrangements.

(3) Maintain the contents of the Telecommunications Forecast, Inventory, and Reporting Database.

(4) Analyze opportunities for sharing dedicated network services and equipment with other USDA agencies.

(b) The Designated Agency Representative/Dedicated (DAR/D) for NRCS is located at the ITC and will:

(1) Order the FTS2001 dedicated network access services upon approval by the TMACO.

(2) Review bills associated with dedicated services.

(c) There are eight NRCS Designated Agency Representative/Non-Dedicated (DAR/N) and for their assigned area will:

(1) Order non-dedicated services and equipment upon approval by the TMACO.

(2) Review bills associated with non-dedicated services and equipment.

(d) Agency Program Managers will:

(1) Document the business needs that require a telecommunications solution.

(2) Review options and the cost/benefit analysis supplied by the TMACO for the proposed telecommunications solution.

(3) Signoff and commit agency funds to procure the selected telecommunications solution.

SUBPART C - VOICE MAIL

512.20 Purpose.

512.21 Policy.

512.22 Definitions.

PART 512 - TELECOMMUNICATIONS MANAGEMENT

SUBPART C - VOICE MAIL

512.20 Purpose.

To establish policy regarding the use of voice mail.

512.21 Policy.

(a) NRCS will provide its employees with a voice mail service to assist them in accomplishing the agency's mission.

(b) Premiere Technologies (VoiceCom) is the mandatory source of supply for voice mail service.

(c) Voice mail will only be used for official communications necessary to carry out the mission of NRCS.

512.22 Definitions.

Voice mail. A computer-based voice message system that allows subscribers to transmit and retrieve voice messages. Voice mail systems are accessed by using a touch-tone telephone.

SUBPART D - LOCAL AREA NETWORK

512.30 Purpose.

512.31 Authorities.

512.32 Policy.

512.33 Definitions.

512.34 Responsibilities.

512.35 Security.

PART 512 - TELECOMMUNICATIONS MANAGEMENT

SUBPART D - LOCAL AREA NETWORK

512.30 Purpose.

To establish the policy for local area networks (LAN).

512.31 Authorities.

Telecommunications and Internet Services and Use, USDA Departmental Regulation (DR) 3300-001, March 1999.

512.32 Policy.

(a) All requests for LAN equipment and software require technical approval in accordance with guidelines in Part 405, Information Technology Technical Approval (TA).

(b) All NRCS LANs will have TCP/IP as the network operating system.

(c) As a minimum, all NRCS LANs will be 10BaseT Ethernet using level 5 unshielded twisted pair wire.

(d) NRCS offices in the Agriculture complex in Washington, D.C., must use the Departmental LAN to transverse floors, wings, or buildings. A request for waiver from using the Departmental LAN must be submitted to Departmental Administration for technical approval.

512.33 Definitions.

Local area network (LAN). A telecommunications system within a specified geographical area designed to allow a number of independent devices to communicate with each other over a common transmission mode. LAN's are generally restricted to small geographical areas (i.e., rooms, buildings, or cluster of buildings) and utilize fairly high data rates.

512.34 Responsibilities.

(a) The NRCS Chief Information Officer will ensure that all NRCS and partnering agency's local area network and wide area network activities are coordinated with the Service Center Interagency Technology Working Group.

(b) The LAN/WAN/Voice Team Leader will:

(1) Manage, deploy, and maintain LAN/WAN/Voice equipment and activities for the USDA Service Center Agencies including NRCS.

(2) Provide budget, performance measures, milestones, and other information to support the NRCS IRM planning process.

512.35 Security.

State offices and regional offices are classified as ADP Security Type 2 installations. Reference Part 502, Security Management, for security and privacy considerations. Facilities with LAN's provide an opportunity for unauthorized system access and are subject to the appropriate security treatment.

SUBPART E - RADIO COMMUNICATIONS

PART 512 - TELECOMMUNICATIONS MANAGEMENT

SUBPART E - RADIO COMMUNICATIONS

512.40 Purpose.

To state NRCS policy and assign responsibility for the management, acquisition, and utilization of two-way radio communications.

512.41 Authorities.

(a) U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA) Manual of Regulations and Procedure for Federal Radio Frequency Management.

(b) Telecommunications and Internet Services and Use, USDA Departmental Regulation (DR) 3300-001, March 1999.

512.42 Policy.

Two-way radio, when properly authorized, may be used in support of the following NRCS activities:

(a) Snow surveys and water supply forecasting. For voice communications between snow survey personnel and for transmitting snow survey and other hydrometerological data from snow sensors to field office base stations and to the SNOTEL minicomputer system.

(b) Engineering and cartographic field surveys. For voice communications between survey party members.

(c) Planning and operations activities under watershed, RC&D, and other project activities. For voice communications between project personnel.

(d) Cooperative ventures with other agencies. For joint use of communication facilities in which NRCS operations are served.

(e) Other activities if specifically approved through National Headquarters on a case-by-case basis.

512.43 Definitions.

Two-way radio communication. Includes Citizens Band Radio Service (CB), radio telemetry (all modes), voice communications systems (all modes), and radio telephone.

512.44 Procedures for Authorization.

(a) The Information Technology Center is responsible for radio communications management NRCS-wide.

(b) The ITC will:

(1) Approve the acquisition (by purchase, lease, or other agreement) of all radio equipment prior to acquiring the equipment. Technical approvals from the Telecommunications Staff are returned to the State office.

(2) Approve the disposal of equipment.

(3) Process frequency and station authorizations received from State offices.

(4) Perform a technical evaluation and, if appropriate, approve the request received from the State office.

(5) Provide technical guidance.

(c) The National Water and Climate Center (NWCC) will approve a request to acquire or dispose of radio equipment to be used for snow survey and water supply forecasting before it is submitted to the ITC. After approval by NWCC, the request will be forwarded to the ITC.

(d) The State office staffs will:

(1) Forward requests for approval of two-way radios to the ITC.

(2) Forward requests for two-way radios for snow survey and water supply forecasting use to the NWCC.

(3) Submit requests for frequency and station authorizations to the ITC.

(4) Submit requests for acquisitions (by purchase, lease, or other agreement) to the ITC prior to acquiring equipment.

512.45 Use and Restrictions.

(a) Citizens band (CB) radio service.

(1) Use of CB radios by Federal agencies is covered by regulations of the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA). The Interdepartmental Radio Advisory Committee (IRAC) must process all CB license and equipment requests. These must be submitted through State offices to the Telecommunications Staff, ITC.

(2) FCC regulations. FCC rules and regulations severely constrain the use of CB frequencies by Federal agencies. FCC will not authorize the use of CB radio for routine Federal business. The following "S-NOTE #348" will be placed on all frequency assignments approved by IRAC for CB radio service:

"Operations are subject to compliance with FCC Rules and Regulations, Part 95, Subpart D. Transmitters may be operated by employees of the federal government only for the purpose of interfacing with non-government licensees to coordinate essential and mutual activities. This authority may be rescinded by FCC in its discretion at any time."

(3) NTIA regulations. NTIA regulations prohibit Federal agencies from acquiring CB equipment unless prior clearance is obtained from IRAC.

(4) IRAC involvement. State offices are to forward requests for CB frequencies and CB equipment to the Telecommunications Staff, ITC, who will route them to IRAC.

(5) Other restrictions. GSA will not authorize the installation of CB radios in interagency motor pool vehicles unless the agency has a valid FCC license authorizing the use of CB frequencies. Under no circumstances are employee-owned or other privately-owned CB radios to be used in NRCS-owned or leased vehicles. FCC will not accept license applications from Federal employees on behalf of USDA agencies. Illegal use of CB equipment in a Federal vehicle can result in revocation of an employee's license, a fine, or both.

(b) Radio telemetry. Radio telemetry may be used to transmit data for snow survey, water supply forecasting, and other hydrometeorological functions.

(c) Voice communications. Radio systems for voice communications may be used if it is determined that:

(1) Normal means of communications are not available;

(2) The efficiency achieved will justify the cost of the system; and

(3) The equipment is needed on a permanent or long-term basis.

(d) Radio telephone. Radio telephone equipment may be acquired for communications from mobile to land telephone stations if other means of communication (cellular telephones) do not exist or are not as practical. Leased radio telephone equipment should be considered if the need is short-term and acquisition of conventional equipment would not be practical. A successful test of such equipment is to be conducted in the planned area of use prior to acquisition.

SUBPART F - TELEPHONE COMMUNICATIONS

512.50 Purpose.

512.51 Authorities.

512.52 Policy.

PART 512 - TELECOMMUNICATIONS MANAGEMENT

SUBPART F - TELEPHONE COMMUNICATIONS

512.50 Purpose.

To establish policy for the acquisition, use, and disposal of telephone systems and related services.

512.51 Authorities.

Telecommunications and Internet Services and Use, USDA Departmental Regulation (DR) 3300-001, March 1999.

512.52 Policy.

(a) Telephone service provided at designated GSA consolidated locations is a non-mandatory source of supply for local telephone service. However, the moving off GSA consolidated service requires a waiver from the Department.

(b) All requests for waivers from GSA consolidated service must be submitted to the NRCS TMACO.

(c) All other requests for telephone systems and related services must be submitted to the NRCS TMACO.

(d) Telephone lines and instruments may be added to existing systems provided the systems changes and quantity thresholds are considered.

(e) Telephone conversations are not to be recorded or monitored.

SUBPART G - FACSIMILE TRANSMISSION

512.60 Purpose.

512.61 Policy.

PART 512 - TELECOMMUNICATIONS MANAGEMENT

SUBPART G - FACSIMILE TRANSMISSION

512.60 Purpose.

To establish policy for the use of facsimile transmission equipment.

512.61 Policy.

(a) Facsimile transmission will only be used for official documents that are time sensitive or that require an immediate response or action.

(b) Sensitive information should not be transmitted by facsimile except in emergency situations. Sensitive considerations include the following information:

(1) Individual cooperators.

(2) The investigation and/or discipline of employees.

(3) The investigation of contractors or potential contractors.

PART 513- INTERNET MANAGEMENT

513.0 Purpose.

513.1 Authorities.

513.2 Policy.

513.3 Definitions.

513.4 Responsibilities.

PART 513- INTERNET MANAGEMENT

513.0 Purpose.

To provide Natural Resources Conservation Service (NRCS) employees and other authorized users at all levels with policy and responsibilities for the management and use of the USDA Internet. Authorized users of NRCS equipment and networks have the same responsibilities in adhering to this policy as do NRCS employees.

513.1 Authorities.

(a) Americans with Disabilities Act of 1990.

(b) Management of Federal Information Resources, Office of Management and Budget (OMB) Circular A-130.

(c) Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995.

(d) Privacy Act of 1974, 5 U.S.C. 552a.

(e) The Rehabilitation Act Amendments of 1992, Public Law 102-569

(f) Home Page Development and Maintenance, USDA Departmental Regulation (DR) 3430-1, August 1995.

(g) Internet Security Policy, USDA Departmental Regulation (DR) 3140-002, March 1995.

513.2 Policy.

(a) NRCS organizations and employees will use the USDA Internet and the world wide web (www) for performing NRCS official business as much as practical.

(b) NRCS employees are agents of the NRCS and USDA. Employees will conduct their business on the USDA Internet and the www in accordance with Federal Information Processing (FIP), security, Freedom of Information Act, and related policies and procedures.

(c) NRCS employees at all levels will use NRCS information systems in a way that is legal and proper and that does not suggest even the appearance of illegality or impropriety in the judgment of a reasonable person.

(d) NRCS employees at all levels who download information from the Internet and NRCS Information Resource Network must ensure that:

(1) Intellectual property rights are protected;

(2) Software and documents contain nothing detrimental to the operation of a NRCS computer system, for example, viruses;

(3) The information downloaded helps the employee fulfill a portion of the agency mission; and

(4) The information is accurate and effective in helping the employee do his or her job.

(e) NRCS will establish partnerships with other organizations to create an effective and efficient network of communication services. NRCS will establish a supporting infrastructure to expedite delivery of information and services to farmers, ranchers, employees, partners, other involved members of the public, and other agencies.

(f) NRCS organizations will establish and maintain services on the USDA Internet, including the world wide web (www). Services must support legitimate mission activities of the NRCS and include prudent operations and security measures.

(g) All NRCS information system resource servers (including www and FTP servers) connected to publicly accessible networks will employ the appropriate security safeguards. See DR-3140-2. Security safeguards will ensure the integrity, authenticity, privacy, and availability of the information system and its data.

(h) NRCS activities will employ suitable security measures to adequately protect the network from unauthorized intrusion and compromising of data or information from internal or external sources. Refer to Part 502, Security Management.

(i) NRCS activities may establish and maintain links from its documents, data, and software to related information belonging to the agency and other USDA and Federal organizations. NRCS will avoid links to commercial businesses, unless there is an NRCS mission related need, and all such links will be prefaced with a disclaimer page stating that the user is leaving NRCS managed www content.

(j) The Management Services Division (MSD) will establish clearance procedures for directives disseminated through the USDA Internet. Clearances are necessary to ensure compliance with required directives management procedures of NRCS, USDA, NARA, and other agencies. The Management Services Division will also establish records management procedures for other official documents from which portions or all of the documents may be replicated for dissemination over the www.

(k) Information provided through the USDA Internet will be current, accurate, maintained, factual, professionally presented, and related to the mission of the NRCS.

(l) All NRCS information resource servers will have a person or staff assigned to administer each service.

(m) Each www system and subsystem (or web site) will have a tracking system or log that includes the names of document authors, information owners, date created, expiration date or disposition, date last reviewed, etc. Contact information such as telephone number, e-mail address, mailing address, and organization will also be included. Because of the variety of types of www services, a single tracking or logging system is not feasible. Administrators will use features of servers and application tools for tracking and logging purposes where possible.

(n) All www systems created or managed by NRCS will accommodate the needs of users with disabilities. Web sites will be designed to perform for a wide variety of browsers.

513.3 Definitions.

(a) Browser. A software application used to locate and display Web pages. The two most popular graphical browsers are Netscape Navigator and Microsoft Internet Explorer. These graphical browsers can display graphics, text, and multimedia information, including sound and video.

(b) Domain Name System (or Service) (DNS). A distributed database system established by the Internet that translates alphabetic (user friendly) domain names into numeric (machine friendly) IP addresses and vice-versa. Every time you use a domain name, a DNS service must translate the name into the corresponding IP address.

(c) Home Page. Primary page or starting point of a collection of Web pages managed as a web site on a single www server.

(d) Internet. A worldwide system for linking smaller computer networks together. Networks connected through the Internet use the TCP/IP protocol to communicate.

(e) Intranet. A Web site or group of Web sites belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web site looks and acts just like any other Web site, but the security measures surrounding an intranet prevent unauthorized access.

(f) Staging Server. A Web server that contains documents and Web applications that are under test or review for approval. Such servers have restricted access to prevent the inadvertent release of draft or pre-publish information to the public or employees.

(g) Production Server. A Web server that contains documents or web applications that have been formally reviewed, tested, and approved for use by the intended audience. A production server may provide restricted access to information for internal use over the USDA intranet or provide anonymous access by the general public.

(h) Uniform Resource Locator (URL). The URL is the address of a web page or directory containing a "home page," i.e., http://www.usda.gov. Every web page must have an address in order for it to be accessed on the Internet.

(i) Webmaster (Web Coordinator). Person(s) who manages a web and ensures that applicable standards are met; optimizes the web architecture for navigability; takes editorial responsibility for the content, quality and style of the site; finds, creates, and installs tools to create web content and to check consistency.

(j) Web Farm. A system of dedicated servers managed at a single location with a uniform set of polices and procedures for content development, management, presentation, testing, and security. Servers included in the farm may include a wide variety of servers for Web pages, database access, file transfer, authentication, and other functions. NRCS maintains web farms at the ITC in Fort Collins, Colorado.

(k) Web Steering Team (WST). The Web Steering Team has the responsibility to guide the development and implementation of agency policy, standards, and guidelines for web-based content. Members include one representative from major organizational levels within the agency.

(l) World Wide Web (www). The Web represents the portion of the Internet that uses HTTP, hypertext transport protocol. Web content is generally presented via HyperText Markup Language (HTML) formatted documents, although some browsers translate Extended Markup Language (XML) documents directly.

513.4 Responsibilities.

(a) The Chief of the Natural Resources Conservation Service will:

(1) Provide support for the agency web site and internet/intranet activities.

(2) Appoint representatives to the Web Steering Committee.

(b) The NRCS Chief Information Officer will:

(1) Ensure that the necessary infrastructure, roles, responsibilities, and resource requirements for the use of Internet and intranets are in place to establish operational capacities. The infrastructure will define persistent or reliable networked information resources, standards, security measures, and operational procedures for the NRCS Web Systems.

(2) Manage and coordinate the development of NRCS Internet policies and procedures.

(3) Ensure the coordination with USDA and Service Center initiatives, e.g., LAN/WAN/Voice, common computing environment, etc.

(4) Establish procedures to ensure that NRCS Web systems comply with USDA and NRCS policies, Federal regulations and executive orders.

(5) Ensure that adequate training and technical support are provided.

(6) Track NRCS expenditures for Internet and Web activities. Prepare recommendations for budget allocations that will procure the best technologies and support necessary to ensure the best delivery of information and services to customers, partners, and employees.

(c) The Conservation Communications Staff Director will:

(1) Provide one or more staff members to manage or coordinate the visual display and organization of the NRCS Home Page and associated web subsystems.

(2) Chair the Web Steering Committee.

(3) Establish procedures to ensure that NRCS Web systems have both content and format that meets the needs of customers, employees, and partners.

(4) Review NRCS Web resources for appropriate use of NRCS web styles and presentation and submit suggested changes to the organizational unit responsible for the web system.

(d) The Information Technology Center Director will:

(1) Host the agency home page and associated top-level web pages on a web server the address of which shall be www.nrcs.usda.gov and provide an assigned system administrator to manage this site on the NRCS Web Farm.

(2) Manage the NRCS Web Farm including all resource servers to provide web hosting services to all levels of NRCS with the authority to create internet and related web resources.

(3) Provide a position of Web Operations Manager to oversee the NRCS Web Farm.

(4) Provide adequate training and staffing for all web administration and management duties associated with the NRCS Web Farm.

(5) Coordinate and implement web standards and security measures with other USDA Internet and www management.

(6) Manage the agency Domain Name System (DNS) and the File Transfer Protocol (FTP) servers.

(7) Evaluate and recommend appropriate www technologies to NRCS.

(8) Develop test procedures and web system requirements that ensure adequate web security and performance of all web systems hosted on the NRCS Web Farm or other web servers.

(9) Develop transition plans to move Web services from isolated Web servers to the NRCS Web Farm when increased security and performance are required.

(e) The Web Operations Manager will:

(1) Provide guidance and assistance to web developers who wish to create or maintain Web services (web sites or applications) on the NRCS web farm.

(2) Implement the policies and procedures necessary to manage the NRCS Web Farm.

(3) Review all Web services for compliance with polices and standards prior to publication or release on NRCS production servers.

(4) Prepare plans and budgets necessary to operate the NRCS Web Farm.

(5) Ensure that all Web Services are adequately tested prior to release on NRCS production servers.

(6) Manage dedicated Web and System Administrator personnel, staff, and contracts necessary for the maintenance and operation of the NRCS Web Farm.

(f) The Web Steering Team Leader will:

(1) Initiate and coordinate NRCS web site activities and draft policies for NRCS homepage development and maintenance.

(2) Develop and coordinate the implementation of a plan to make the www a mainstream way of doing e-business with employees, customers, and partners by making the NRCS web systems behave as an integrated, consistent method for delivering information and services.

(3) Coordinate the design and development of an enterprise-wide web system including the designation of dedicated Web systems designed for internal uses, external uses, specific subject areas, and description of organizational units.

(4) Coordinate the use of common procedures and methods on the enterprise-wide web system including the use of common search tools, web page templates, and development tools.

(g) Web Developers will:

(1) Follow all USDA and NRCS Internet/www policies.

(2) Submit web systems to test procedures developed by the ITC.

(3) Obtain appropriate reviews and approval of web content from the organizational unit responsible for the content of the web system.

PART 514 - ELECTRONIC EQUIPMENT ACCESSIBILITY BY EMPLOYEES WITH DISABILITY

514.0 Purpose.

514.1 Authorities.

514.2 Policy.

514.3 Definitions.

514.4 Responsibilities.

PART 514 - ELECTRONIC EQUIPMENT ACCESSIBILITY BY EMPLOYEES WITH DISABILITIES

514.0 Purpose.

To provide policy and responsibilities for complying with Federal and USDA policies for the electronic equipment accommodation of employees with disabilities. These policies and responsibilities apply to all NRCS offices nationwide.

514.1 Authorities.

(a) The Rehabilitation Act Amendments of 1992, Public Law 102-569.

(b) Disability Employment Program, NRCS General Manual 230-403 E.

(c) USDA TARGET Center Publication, “The Accessible Resources Center."

(d) Workforce Investment Act: Section 508 Electronic and Information Technology.

514.2 Policy.

(a) NRCS, through its Disability Employment Program and USDA TARGET Center services, will ensure that NRCS employees with disabilities have access to electronic office equipment, including computer and communications technology as necessary to perform job duties unless an undue burden would be imposed on the agency.

(b) NRCS encourages the employment of persons with disabilities in accordance with the National Disability Employment Program.

(c) NRCS will provide guidance and assistance to NRCS managers and supervisors on their responsibilities in the employment of persons with disabilities.

514.3 Definitions.

USDA TARGET Centers. A USDA facility located at USDA Headquarters and at St. Louis, Missouri. It provides consultation, assessment, and evaluation services to USDA employees nationwide regarding electronic equipment accommodations that may aid employees with disabilities to better perform their job functions. The Target Centers:

(a) Provide leadership in the evaluation, assessment, and application of information technology for the use of USDA employees with disabilities.

(b) Provide contract clauses that address accommodating equipment needs for use in solicitations and contracts.

(c) Telephone numbers to contact the TARGET Centers are:

(1) USDA Headquarters, (202) 720-2600 (Voice/TDD/TTY).

(2) USDA St. Louis facility, (314) 539-3800 (Voice/TDD/TTY).

514.4 Responsibilities.

(a) The NRCS National Disabled Employment Program (DEP) Manager and local DEP managers will provide assistance and guidance to NRCS managers and supervisors on the employment of persons with disabilities and on the accessibility to accommodating information technology equipment by qualified employees.

(b) Supervisors and line managers will:

(1) Ensure that accommodating information technology equipment is available for use by qualified employees.

(2) Allocate funds for the acquisition of information technology equipment for employees with disabilities.

(c) Information Technology staffs NRCS-wide will:

(1) Assist the DEP Manager or NRCS managers and supervisors in obtaining TARGET Center assessments of employees who may benefit from electronic equipment accommodation.

(2) Assist in the acquisition, installation, operation, and maintenance of accommodating hardware, software, and peripherals.

PART 515 - INFORMATION RESOURCES MANAGEMENT REVIEWS

PART 515 - INFORMATION RESOURCES MANAGEMENT REVIEWS

515.0 Purpose

To establish policy for conducting reviews of major information systems and their management within the Natural Resources Conservation Service (NRCS). Reviews are conducted to ensure that management functions and practices are in compliance with established Departmental and external policies, principles, standards, and guidelines.

515.1 Authorities.

(a) Computer Security Act of 1987, Public Law 100-235.

(b) Federal Manager's Financial Integrity Act of 1982.

(c) Management Accountability and Control, Office of Management and Budget (OMB) Circular A-123.

(d) Financial Management Systems, Office of Management and Budget (OMB) Circular A-127.

(e) Management of Federal Information Resources, OMB Circular A-130.

(f) Paperwork Reduction Reauthorization Act of 1986, Public Law 99-500.

(g) Title 44 United States Code (Government Printing and Binding Regulations).

(h) Acquisition of IRM Resources, USDA Departmental Regulation (DR) 3130-001, September 1995.

(i) IRM Review Program, USDA Departmental Regulation (DR) 3150-002, January 1989.

515.2 Policy.

(a) NRCS will review its major information systems once every (2) two years.

(b) NRCS will follow information systems review requirements and processes set forth in USDA Departmental Regulation 3150-002.

515.3 Definitions.

(a) Major Information System. Major information systems are information systems that are:

(1) Crucial to an agency's mission; or

(2) Significant to the administration of agency programs, finances, property, or other resources.

(3) More specifically to NRCS, the systems reported to the Department in the IRM Long-Range Plan.

(b) Selective Review. Review of an USDA agency automated system, or project, or its IRM management. Selective reviews are conducted on-site, performed jointly by OIRM and the agency to produce an assessment of the system and its management.

(c) Self-Review. An IRM review which an agency conducts on one or more of its IRM systems, organizations, or activities.

515.4 Responsibilities.

(a) The NRCS Chief Information Officer will ensure that an effective information resources management review program is established and followed.

(b) The Operations Management and Oversight Division Director will provide guidance to the Regional Oversight and Evaluation Team and NRCS managers on all oversight and reviews, including major application information system reviews.

(c) The Regional Oversight Evaluation Team Leader will work with other regional teams to establish strategies to ensure the review of major information systems.

(d) NRCS managers will implement oversight and reviews under national policy guidelines, including major information systems reviews.

PART 516 - IRM TRAINING AND EMPLOYEE DEVELOPMEN

516.0 Purpose.

516.1 Authorities.

516.2 Responsibilities.

PART 516 - IRM TRAINING AND EMPLOYEE DEVELOPMENT

516.0 Purpose.

To provide policy and responsibilities for IRM training and employee development.

516.1 Authorities.

(a) Information Technology Management Reform Act (ITMRA) of 1996 (Clinger-Cohen Act of 1996).

(b) "Using Technology to Improve Training Opportunities for Federal Government Employees, " Executive Order 13111, January 12, 1999.

(c) NRCS General Manual (GM) 360, Part 410, Employee Development Program, Amendment 54, March 1991.

(d) "Clinger-Cohen Core Competencies," Education and Training Committee, Chief Information Council.

516.2 Responsibilities.

(a) The NRCS Chief Information Officer will:

(1) Provide leadership in the development of an annual NRCS IRM employee training plan.

(2) Coordinate national IRM employee development requirements including core competencies, proficiency models, etc., and advertise potential sources that meet these requirements, working with National Employee Development Center (NEDC), as appropriate.

(3) Designate an NRCS IRM training coordinator who is responsible for national IRM training and development needs, working with NEDC as appropriate.

(b) The NRCS IRM Training Coordinator will:

(1) Determine what IRM training will best meet the needs of NRCS employees by working with State, Regional, NHQ, and Consortium IRM training committees, the Information Technology Center and others as appropriate.

(2) Determine the best method of providing training to employees by working with the NEDC, coordinating efforts with IRM training committees and coordinators.

(3) Prepare annual training inventory and needs report to the Chief Information Officer to integrate into the annual NRCS IRM Employee Training Plan.

(c) The Information Technology Center (ITC) Director will work with NEDC and the training coordinator to design and develop IRM courses and training related to software development, implementation, and deployment.

(d) Regional Conservationists, State Conservationists, division directors, center directors, and institute directors will:

(1) Provide leadership in identifying IRM training needs and sources to satisfy these needs.

(2) Designate, as appropriate, an IRM training coordinator.

(3) Ensure that technical specialists (e.g., soil scientist, biologists) receive training on business applications.